

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2 0 0 4 年 4 月 1 5 日

出 願 番 号

Application Number:

特 願 2 0 0 4 - 1 2 0 1 3 2

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 2 0 0 4 - 1 2 0 1 3 2

出 願 人

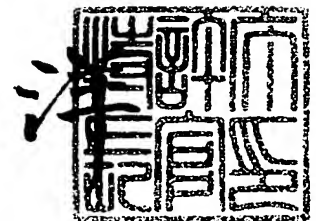
Applicant(s):

松下電器産業株式会社

2 0 0 5 年 5 月 2 0 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



BEST AVAILABLE COPY

【官 公 庁】

付 付 願

【整理番号】

2047960017

【提出日】

平成16年 4月15日

【あて先】

特許庁長官殿

【国際特許分類】

G06F 15/177

【発明者】

【住所又は居所】

大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】

張 毅波

【発明者】

【住所又は居所】

大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】

古門 健

【特許出願人】

【識別番号】

000005821

【氏名又は名称】

松下電器産業株式会社

【代理人】

【識別番号】

100097445

【弁理士】

【氏名又は名称】

岩橋 文雄

【選任した代理人】

【識別番号】

100103355

【弁理士】

【氏名又は名称】

坂口 智康

【選任した代理人】

【識別番号】

100109667

【弁理士】

【氏名又は名称】

内藤 浩樹

【手数料の表示】

【予納台帳番号】

011305

【納付金額】

16,000円

【提出物件の目録】

【物件名】

特許請求の範囲 1

【物件名】

明細書 1

【物件名】

図面 1

【物件名】

要約書 1

【包括委任状番号】

9809938

【請求項 1】

第 1 の通信装置と第 2 の通信装置を含むネットワークにおいて第 2 の通信装置の認証を行う認証システムであって、

前記第 1 の通信装置は表示部と認証入力部を備え、

前記第 2 の通信装置には、予め認証に使用する ID 情報の付与が可能であり、

前記第 2 の通信装置から前記第 1 の通信装置に対して接続要求を行い、

前記第 2 の通信装置から前記第 1 の通信装置に対して前記 ID 情報を送信して認証要求を行い、

前記第 1 の通信装置が、受信した前記 ID 情報を前記表示部に表示し、

前記認証入力部への入力に従って、前記第 1 の通信装置が認証成功を前記第 2 の通信装置に通知し、

ユーザが前記表示部に表示された ID 情報に基づき前記認証入力部を操作して認証許可不許可判断を行うことを可能にしたことを特徴とする認証システム。

【請求項 2】

第 1 の通信装置、第 2 の通信装置および第 3 の通信装置を含むネットワークにおいて第 2 の通信装置の認証を行う認証システムであって、

前記第 3 の通信装置は表示部と認証入力部を備え、

前記第 2 の通信装置には、予め認証に使用する ID 情報の付与が可能であり、

前記第 2 の通信装置から前記第 1 の通信装置に対して接続要求を行い、

前記第 2 の通信装置から前記第 1 の通信装置に対して前記 ID 情報を送信して認証要求を行い、

前記第 1 の通信装置が、前記認証要求に対応して、前記第 3 の通信装置に前記 ID 情報を送信して認証要求を依頼し、

前記第 3 の通信装置が、受信した前記 ID 情報を前記表示部に表示し、

前記認証入力部への入力に従って、前記第 3 の通信装置が認証成功を前記第 1 の通信装置に通知し、

前記第 1 の通信装置が、前記第 3 の通信装置から通知された認証成功を、前記第 2 の通信装置に通知し、

ユーザが前記表示部に表示された ID 情報に基づき前記認証入力部を操作して認証許可不許可判断を行うことを可能にしたことを特徴とする認証システム。

【請求項 3】

第 1 の通信装置と第 2 の通信装置を含むネットワークにおいて第 2 の通信装置の認証を行う認証システムであって、

前記第 1 および第 2 の通信装置は暗号鍵選択部と複数の暗号鍵を記憶する記憶部をそれぞれ備え、

前記第 1 の通信装置において前記暗号鍵選択部が前記複数の暗号鍵から 1 つを選択し、

前記第 2 の通信装置において前記暗号鍵選択部が前記複数の暗号鍵から 1 つを選択し、

前記第 2 の通信装置から前記第 1 の通信装置に対して接続要求を行い、

前記第 2 の通信装置から前記第 1 の通信装置に対して認証要求を行い、

前記第 1 の通信装置が、前記第 2 の通信装置に対してチャレンジを伴う第 1 の認証応答を行い、

前記第 2 の通信装置が、自身が選択した暗号鍵を用いて、前記チャレンジの内容を暗号化して、前記第 1 の通信装置に対して第 2 の認証応答を行い、

前記第 1 の通信装置が、自身が選択した暗号鍵を用いて、前記暗号化されたチャレンジを復号化し、送信したチャレンジと一致する場合、前記第 2 の通信装置に認証成功を通知し、

ユーザが前記第 1 の通信装置と前記第 2 の通信装置において同一の暗号鍵を選択した場合に、前記第 1 の通信装置により前記第 2 の通信装置の認証が行われるようにしたことを特徴とする認証システム。

【請求項 4】

- ・ 第 1 の通信装置、第 2 の通信装置および前記第 3 の通信装置を含むネットワークにおいて第 2 の通信装置の認証を行う認証システムであって、
- ・ 前記第 2 および第 3 の通信装置は暗号鍵選択部と複数の暗号鍵を記憶する記憶部をそれぞれ備え、
 - 前記第 2 の通信装置において前記暗号鍵選択部が前記複数の暗号鍵から 1 つを選択し、
 - 前記第 3 の通信装置において前記暗号鍵選択部が前記複数の暗号鍵から 1 つを選択し、
 - 前記第 2 の通信装置から前記第 1 の通信装置に対して接続要求を行い、
 - 前記第 2 の通信装置から前記第 1 の通信装置に対して認証要求を行い、
 - 前記第 1 の通信装置が前記認証要求を前記第 3 の通信装置に転送し、
 - 前記第 3 の通信装置が、前記第 1 の通信装置に対してチャレンジを伴う第 1 の認証応答を行い、
 - 前記第 1 の通信装置が、受信した前記チャレンジを伴う第 1 の認証応答を前記第 2 の通信装置に転送し、
 - 前記第 2 の通信装置が、自身が選択した暗号鍵を用いて、受信した前記チャレンジの内容を暗号化して、前記第 1 の通信装置に対して第 2 の認証応答を行い、
 - 前記第 1 の通信装置が、前記第 2 の認証応答を前記第 3 の通信装置に転送し、
 - 前記第 3 の通信装置が、自身が選択した暗号鍵を用いて、受信した前記暗号化されたチャレンジを復号化し、送信したチャレンジと一致する場合、前記第 1 の通信装置に認証成功を通知し、
 - 前記第 1 の通信装置が、前記認証成功を前記第 2 の通信装置に転送し、
- ユーザが前記第 2 の通信装置と前記第 3 の通信装置において同一の暗号鍵を選択した場合に、前記第 3 の通信装置により前記第 2 の通信装置の認証が行われるようにしたことを特徴とする認証システム。

【請求項 5】

前記認証が成功した後に、前記第 1 の通信装置と前記第 2 の通信装置の間で通信接続を行うことを特徴とする請求項 1 乃至 4 何れか一項記載の認証システム。

【請求項 6】

前記第 1 の通信装置と前記第 2 の通信装置は、無線 LAN 規格に従って通信を行うことを特徴とする請求項 1 乃至 4 何れか一項記載の認証システム。

【請求項 7】

前記第 1 の通信装置がアクセスポイント装置であるか、前記第 2 の通信装置がクライアント装置であるか、アクセスポイント装置であるか、または、リピータ装置であることを特徴とする請求項 1 乃至 4 何れか一項記載の認証システム。

【請求項 8】

前記第 3 の通信装置は、ルータ装置であることを特徴とする請求項 2 または 4 何れか記載の認証システム。

【請求項 9】

前記 ID 情報は、前記第 2 の通信装置が複数ある場合、前記ネットワーク内の前記第 2 の通信装置に共通で且つユーザだけが知っている識別情報、または、前記第 2 の通信装置毎に付与された前記第 2 の通信装置を識別する ID 情報であって、ユーザが知っている ID 情報であることを特徴とする請求項 1 または 2 記載の認証システム。

【請求項 10】

前記第 2 の通信装置には、自身が識別される ID 情報が付与されており、前記第 1 の通信装置に認証を要求する場合、自身の ID 情報を前記第 1 の通信装置に知らせ、前記第 1 の通信装置は、認証済みの前記第 2 の通信装置の前記 ID 情報を、認証済み ID 情報として記憶しておき、以降、前記第 1 の通信装置は、認証要求を受けた場合、受信した ID 情報が前記認証済み ID 情報かどうか調べ、認証済みの場合、認証済み処理手順として、前記認証入力部への入力の有無にかかわらず、認証成功を前記第 2 の通信装置に通知することを特徴とする請求項 1 記載の認証システム。

【請求項 1 1】

前記第 2 の通信装置には、自身が識別される ID 情報が付与されており、前記第 1 の通信装置に認証を要求する場合、自身の ID 情報を前記第 1 の通信装置に知らせ、前記第 1 の通信装置は前記 ID 情報を前記第 3 の通信装置に転送し、前記第 3 の通信装置は、認証済みの前記第 2 の通信装置の前記 ID 情報を認証済み ID 情報として記憶しておき、以降、認証要求を受けた場合、受信した ID 情報が前記認証済み ID 情報かどうか調べ、調べた結果が認証済みの場合、認証済み処理手順として、前記認証入力部への入力の有無にかかわらず、前記第 3 の通信装置は、認証成功を前記第 1 の通信装置を経由して前記第 2 の通信装置に通知することを特徴とする請求項 2 記載の認証システム。

【請求項 1 2】

前記第 2 の通信装置には、自身が識別される ID 情報が付与されており、前記第 1 の通信装置に認証を要求する場合、自身の ID 情報を前記第 1 の通信装置に知らせ、前記第 1 の通信装置は、認証済みの前記第 2 の通信装置の前記 ID 情報を認証済み ID 情報として記憶しておき、以降、認証要求を受けた場合、受信した ID 情報が前記認証済み ID 情報かどうか調べ、認証済みの場合には、認証済み処理手順として、前記第 1 の通信装置および前記第 2 の通信装置における前記暗号鍵の選択の有無、前記第 1 の認証応答の有無、前記第 2 の認証応答の有無、および、前記暗号化されたチャレンジを復号化し、送信したチャレンジとの一致を判定する動作の有無、にかかわらず、前記第 1 の通信装置は、認証成功を前記第 2 の通信装置に通知することを特徴とする請求項 3 記載の認証システム。

【請求項 1 3】

前記第 2 の通信装置には、自身が識別される ID 情報が付与されており、前記第 1 の通信装置に認証を要求する場合、自身の ID 情報を前記第 1 の通信装置に知らせ、前記第 1 の通信装置は前記 ID 情報を前記第 3 の通信装置に転送し、前記第 3 の通信装置は、認証済みの前記第 2 の通信装置の前記 ID 情報を認証済み ID 情報として記憶しておき、以降、認証要求を受けた場合、受信した ID 情報が前記認証済み ID 情報かどうか調べ、認証済みの場合には、認証済み処理手順として、前記第 2 の通信装置および前記第 3 の通信装置における前記暗号鍵の選択の有無、前記第 1 の認証応答および前記第 1 の認証応答の転送の有無、前記第 2 の認証応答および前記第 2 の認証応答の転送の有無、および、前記暗号化されたチャレンジを復号化し、送信したチャレンジとの一致を判定する動作の有無、にかかわらず、前記第 3 の通信装置は、認証成功を前記第 1 の通信装置を経由して前記第 2 の通信装置に通知することを特徴とする請求項 4 記載の認証システム。

【請求項 1 4】

前記第 1 の通信装置が複数ある場合であって、前記第 1 の通信装置自身が記憶する認証済み ID 情報の中に、認証要求を受け付けた ID 情報が含まれていない場合、自身以外の第 1 の通信装置に問い合わせ、自身以外の第 1 の通信装置の何れかにおいて認証済みの場合、前記認証済み処理手順を行うことを特徴とする請求項 1 0 または 1 2 記載の認証システム。

【請求項 1 5】

前記第 1 の通信装置が複数ある場合であって、各第 1 の通信装置は、自身で認証した認証済み ID 情報を他の第 1 の通信装置に通知して、各第 1 の通信装置が、全認証済み ID 情報を記憶するようにし、前記第 1 の通信装置の何れかが、前記第 2 の通信装置から認証要求を受け付けた場合、自身が記憶する認証済み ID 情報に、認証要求を受け付けた ID 情報が含まれている場合、前記認証済み処理手順を行うことを特徴とする請求項 1 0 または 1 2 記載の認証システム。

【請求項 1 6】

前記第 1 の通信装置が複数ある場合であって、各第 1 の通信装置は、自身で認証した認証済み ID 情報を前記第 3 の通信装置に通知し、前記第 3 の通信装置が全認証済み ID 情報を記憶するようにし、前記第 1 の通信装置の何れかが、前記第 2 の通信装置から認証要求を受け付けた場合、受け付けた前記 ID 情報を前記第 3 の通信装置に通知して認証済み ID 情報かどうか判定し、認証済みと判定された場合、前記認証済み処理手順を行うことを

付図として請求項 1 1 または 1 6 記載の認証システム。

【請求項 1 7】

前記第 2 の通信装置に接続切断モード選択部を設け、ユーザが前記接続切断モードを選択すると、切断電文が前記第 1 の通信装置に送信され、前記ネットワーク内の装置が記憶している認証済み ID 情報から前記第 2 の通信装置の ID 情報を消去することを特徴とする請求項 1 0 乃至 1 6 何れか一項記載の認証システム。

【請求項 1 8】

前記第 1 の通信装置、または、前記第 3 の通信装置に、認証済み ID 情報を表示できる表示部と、表示された認証済み ID 情報の何れかを削除する操作部を設け、前記ネットワーク内の装置が記憶している認証済み ID 情報から所定の前記第 2 の通信装置の認証を解除することができるようにしたことを特徴とする請求項 1 0 乃至 1 6 何れか一項記載の認証システム。

【請求項 1 9】

前記第 2 の通信装置が複数あり、同時に認証要求できる認証システムであって、前記複数の第 2 の通信装置において、それぞれの前記暗号鍵選択部により前記複数の暗号鍵から同一の暗号鍵を選択することにより、前記複数の第 2 の通信装置が、並列して認証されることを特徴とする請求項 3 または 4 記載の認証システム。

【請求項 2 0】

前記表示部と前記認証入力部をリモコン装置上に設け、前記第 1 の通信装置と前記リモコン装置との間に通信路を設け、ユーザが手元で、認証入力を行うようにしたことを特徴とする請求項 1 記載の認証システム。

【請求項 2 1】

前記表示部と前記認証入力部をリモコン装置上に設け、前記第 3 の通信装置と前記リモコン装置との間に通信路を設け、ユーザが手元で、認証入力を行うようにしたことを特徴とする請求項 2 記載の認証システム。

【請求項 2 2】

前記暗号選択部をリモコン装置上に設け、前記第 1 の通信装置と前記リモコン装置との間に通信路を設け、ユーザが手元で、前記暗号鍵選択部により前記複数の暗号鍵から 1 つを選択するようにしたことを特徴とする請求項 3 記載の認証システム。

【請求項 2 3】

前記暗号選択部をリモコン装置上に設け、前記第 3 の通信装置と前記リモコン装置との間に通信路を設け、ユーザが手元で、前記暗号鍵選択部により前記複数の暗号鍵から 1 つを選択するようにしたことを特徴とする請求項 4 記載の認証システム。

【請求項 2 4】

請求項 1 乃至請求項 2 3 何れか一項記載の前記第 1 の通信装置または前記第 2 の通信装置または前記第 3 の通信装置。

【請求項 2 5】

複数の通信装置からなるネットワークにおいて、第 1 の通信装置が第 2 の通信装置の認証を行うシステムであって、

前記第 1 の通信装置は、本体部とリモコン装置を備え、リモコン装置は、本体部と着脱可能に構成され、

前記リモコン装置は、認証用の操作部及び表示部を備え、

前記本体部と前記リモコン装置との間に無線通信路を設け、

前記リモコン装置を前記本体部から外す際に、共有鍵を設定し、

前記リモコン装置を前記本体部から外した状態において、前記共有鍵を使用して、前記操作部及び表示部に関わる情報を暗号化通信することを特徴とする認証システム。

【発明の名称】 認証システムおよび認証用の装置

【技術分野】

【0001】

本発明は無線LANの接続におけるセキュリティ向上と設定の簡単化を両立するのに適した認証と設定の方法及び認証システムに関するものである。

【背景技術】

【0002】

近年、無線LAN技術の進歩が進み、それに伴い普及が進んでいる。有線LANに比べ、面倒な配線問題がないため、家庭内でも普及の兆しが見えてきている。しかし、無線LANは、繋ぐだけで接続できる有線LANと違い、接続のための設定が必要である。無線LANの必須項目であるセキュリティに関する設定を行うと、設定がより一層複雑化してしまい、専門家でない一般ユーザにとっては、困難な作業となってしまう。家庭内で無線LANの普及のために、設定簡単化というのは避けて通れない課題の一つになっている。従来の設定画面を使用する手動設定より、ボタン操作による自動設定のほうが望ましい。簡単な自動設定としてボタン一つ押すだけで設定を行う方法がある。以下に、このような設定方法を2つ説明する。

【0003】

方法（イ）では、有線通信手段、即ち有線Ethernet（R）、を用いて設定を行う。設定を開始するとき、設定選択ボタンを「自動」側に入れるだけで、設定が自動で完了する。この方法では、APとクライアントの間に有線で接続しており、互いの通信関係が既に存在している。そのため、APとクライアントとの間において相手のアイデンティティを確認すること所謂相互認証を行う必要はない。よって、暗号鍵を含むセキュリティ情報の入力／設定を行う必要もない。また、有線通信手段を家庭内のLANで使用する場合、LANが家庭内で閉じているため、通信経路のセキュリティが確保され、その通信経路を通して設定のための接続パラメータのやりとりも当然セキュアとなる。

【0004】

方法（ロ）は、無線通信手段を用いる。APとクライアントとの間で相互認証を行うために、両方に設置されているボタンを同時に押して双方の無線出力パワーを下げ、特別な設定モードに入って、自動的に設定を行う。こうして、一回に設定・接続できるのは位置が最も近い一台である。本方法では、前記のように無線出力パワーをコントロールすることを特徴として、APとクライアントの間に一種の秘密通信の形で、相互認証と設定を行う。表示部を通してユーザによる確認をしないまま相互認証が自動で行われてしまう。また、相互接続するために、APとクライアントと両方において同じ設定モード及びその技術の実装が必要である。別言すれば、中で一つがそれを実装しないと、相互接続ができない。また、一回一台のクライアントしか設定・接続できない（非特許文献1参照）。

【非特許文献1】 “バッファロー 無線LANの設定を簡素化する技術を発表”、日経パソコン 2003年11月24日号、P. 22

【発明の開示】

【発明が解決しようとする課題】

【0005】

しかしながら、前記方法（イ）を無線LANに適用しようとする、接続設定のために、有線インターフェイスを設置することが必要であり、ハードウェアとソフトウェア両方コストがかかる。接続設定だけのために、有線インターフェイスを設置するのは不経済であるので、接続設定もできるだけ無線LAN自身のインターフェイスを用いることが望ましい。

【0006】

一方、前記方法（ロ）では、無線LAN自身のインターフェイスを用いることができるが、無線出力パワーを下げることでAPとクライアント間の秘密通信ができるという仕組みになっている。このような秘密通信で本当にセキュリティを確保できるとは言えない。

例えば、同じ技術を用いて電線が通る範囲にある同種無線LANインターフェイスへで表示している隣家のネット家電と接続してしまう危険を完全非排除することが出来ない。偶然、隣家で同じ設定を行っている可能性があるからである。また、接続上のセキュリティを考慮したため、同時、複数台のクライアントとの設定・接続ができない。さらに、特別専用の認証・設定モードのみ提供しているため、相互接続性が十分ではない。

【0007】

本発明は、前記従来の課題を解決するもので、認証・設定において無線LANインターフェイスを用い、セキュリティと、設定・接続の効率と、相互接続性とが向上した無線LAN認証と設定の方法及びシステムを提供することを目的とする。

【課題を解決するための手段】

【0008】

前記従来の課題を解決するために、本発明の認証システムは、以下のような構成及び動作を採用する。

【0009】

(1) 第1の通信装置と第2の通信装置を含むネットワークにおいて第2の通信装置の認証を行う認証システムであって、前記第1の通信装置は表示部と認証入力部を備え、前記第2の通信装置には、予め認証に使用するID情報の付与が可能であり、前記第2の通信装置から前記第1の通信装置に対して接続要求を行い、前記第2の通信装置から前記第1の通信装置に対して前記ID情報を送信して認証要求し、前記第1の通信装置が、受信した前記ID情報を前記表示部に表示し、前記認証入力部への入力に従って、前記第1の通信装置が認証成功を前記第2の通信装置に通知し、ユーザが前記表示部に表示されたID情報に基づき前記認証入力部を操作して認証許可不許可判断を行うことを可能にしたことを特徴とする認証システム。

【0010】

(2) 第1の通信装置、第2の通信装置および第3の通信装置を含むネットワークにおいて第2の通信装置の認証を行う認証システムであって、前記第3の通信装置は表示部と認証入力部を備え、前記第2の通信装置には、予め認証に使用するID情報の付与が可能であり、前記第2の通信装置から前記第1の通信装置に対して接続要求し、前記第2の通信装置から前記第1の通信装置に対して前記ID情報を送信して認証要求し、前記第1の通信装置が、前記認証要求に対応して、前記第3の通信装置に前記ID情報を送信して認証要求を依頼し、前記第3の通信装置が、受信した前記ID情報を前記表示部に表示し、前記認証入力部への入力に従って、前記第3の通信装置が認証成功を前記第1の通信装置に通知し、前記第1の通信装置が、前記第3の通信装置から通知された認証成功を、前記第2の通信装置に通知し、ユーザが前記表示部に表示されたID情報に基づき前記認証入力部を操作して認証許可不許可判断を行うことを可能にしたことを特徴とする認証システム。

【0011】

(3) 第1の通信装置と第2の通信装置を含むネットワークにおいて第2の通信装置の認証を行う認証システムであって、前記第1および第2の通信装置は暗号鍵選択部と複数の暗号鍵を記憶する記憶部をそれぞれ備え、前記第1の通信装置において前記暗号鍵選択部が前記複数の暗号鍵から1つを選択し、前記第2の通信装置において前記暗号鍵選択部が前記複数の暗号鍵から1つを選択し、前記第2の通信装置から前記第1の通信装置に対して接続要求を行い、前記第2の通信装置から前記第1の通信装置に対して認証要求を行い、前記第1の通信装置が、前記第2の通信装置に対してチャレンジを伴う第1の認証応答を行い、前記第2の通信装置が、自身が選択した暗号鍵を用いて、前記チャレンジの内容を暗号化して、前記第1の通信装置に対して第2の認証応答を行い、前記第1の通信装置が、自身が選択した暗号鍵を用いて、前記暗号化されたチャレンジを復号化し、送信したチャレンジと一致する場合、前記第2の通信装置に認証成功を通知し、ユーザが前記第1の通信装置と前記第2の通信装置において同一の暗号鍵を選択した場合に、前記第1の通信装置により前記第2の通信装置の認証が行われるようにしたことを特徴とする認証シ

【0012】

(4) 第1の通信装置、第2の通信装置および前記第3の通信装置を含むネットワークにおいて第2の通信装置の認証を行う認証システムであって、前記第2および第3の通信装置は暗号鍵選択部と複数の暗号鍵を記憶する記憶部をそれぞれ備え、前記第2の通信装置において前記暗号鍵選択部が前記複数の暗号鍵から1つを選択し、前記第3の通信装置において前記暗号鍵選択部が前記複数の暗号鍵から1つを選択し、前記第2の通信装置から前記第1の通信装置に対して接続要求を行い、前記第2の通信装置から前記第1の通信装置に対して認証要求を行い、前記第1の通信装置が前記認証要求を前記第3の通信装置に転送し、前記第3の通信装置が、前記第1の通信装置に対してチャレンジを伴う第1の認証応答を行い、前記第1の通信装置が、受信した前記チャレンジを伴う第1の認証応答を前記第2の通信装置に転送し、前記第2の通信装置が、自身が選択した暗号鍵を用いて、受信した前記チャレンジの内容を暗号化して、前記第1の通信装置に対して第2の認証応答を行い、前記第1の通信装置が、前記第2の認証応答を前記第3の通信装置に転送し、前記第3の通信装置が、自身が選択した暗号鍵を用いて、受信した前記暗号化されたチャレンジを復号化し、送信したチャレンジと一致する場合、前記第1の通信装置に認証成功を通知し、前記第1の通信装置が、前記認証成功を前記第2の通信装置に転送し、ユーザが前記第2の通信装置と前記第3の通信装置において同一の暗号鍵を選択した場合に、前記第3の通信装置により前記第2の通信装置の認証が行われるようにしたことを特徴とする認証システム。

【0013】

(5) 前記認証が成功した後に、前記第1の通信装置と前記第2の通信装置の間で通信接続を行うことを特徴とする(1)乃至(4)何れか記載の認証システム。

【0014】

(6) 前記第1の通信装置と前記第2の通信装置は、無線LAN規格に従って通信を行うことを特徴とする(1)乃至(4)何れか記載の認証システム。

【0015】

(7) 前記第1の通信装置がアクセスポイント装置であるか、前記第2の通信装置が、クライアント装置であるか、アクセスポイント装置であるか、または、リピータ装置であることを特徴とする(1)乃至(4)何れか記載の認証システム。

【0016】

(8) 前記第3の通信装置は、ルータ装置であることを特徴とする(2)または(4)何れか記載の認証システム。

【0017】

(9) 前記ID情報は、前記第2の通信装置が複数ある場合、前記ネットワーク内の前記第2の通信装置に共通で且つユーザだけが知っている識別情報、または、前記第2の通信装置毎に付与された前記第2の通信装置を識別するID情報であって、ユーザが知っているID情報であることを特徴とする(1)または(2)何れか記載の認証システム。

【0018】

(10) 前記第2の通信装置には、自身が識別されるID情報が付与されており、前記第1の通信装置に認証を要求する場合、自身のID情報を前記第1の通信装置に知らせ、前記第1の通信装置は、認証済みの前記第2の通信装置の前記ID情報を、認証済みID情報として記憶しておき、以降、前記第1の通信装置は、認証要求を受けた場合、受信したID情報が前記認証済みID情報かどうか調べ、認証済みの場合、認証済み処理手順として、前記認証入力部への入力の有無にかかわらず、認証成功を前記第2の通信装置に通知することを特徴とする(1)記載の認証システム。

【0019】

(11) 前記第2の通信装置には、自身が識別されるID情報が付与されており、前記第1の通信装置に認証を要求する場合、自身のID情報を前記第1の通信装置に知らせ、前記第1の通信装置は前記ID情報を前記第3の通信装置に転送し、前記第3の通信装置

は、認証済みの前記第2の通信装置の前記ID情報を認証済みID情報として記憶しておき、以降、認証要求を受けた場合、受信したID情報が前記認証済みID情報かどうか調べ、調べた結果が認証済みの場合、認証済み処理手順として、前記認証入力部への入力の有無にかかわらず、前記第3の通信装置は、認証成功を前記第1の通信装置を経由して前記第2の通信装置に通知することを特徴とする(2)記載の認証システム。

【0020】

(12)前記第2の通信装置には、自身が識別されるID情報が付与されており、前記第1の通信装置に認証を要求する場合、自身のID情報を前記第1の通信装置に知らせ、前記第1の通信装置は、認証済みの前記第2の通信装置の前記ID情報を認証済みID情報として記憶しておき、以降、認証要求を受けた場合、受信したID情報が前記認証済みID情報かどうか調べ、認証済みの場合には、認証済み処理手順として、前記第1の通信装置および前記第2の通信装置における前記暗号鍵の選択の有無、前記第1の認証応答の有無、前記第2の認証応答の有無、および、前記暗号化されたチャレンジを復号化し、送信したチャレンジとの一致を判定する動作の有無、にかかわらず、前記第1の通信装置は、認証成功を前記第2の通信装置に通知することを特徴とする(3)記載の認証システム。

【0021】

(13)前記第2の通信装置には、自身が識別されるID情報が付与されており、前記第1の通信装置に認証を要求する場合、自身のID情報を前記第1の通信装置に知らせ、前記第1の通信装置は前記ID情報を前記第3の通信装置に転送し、前記第3の通信装置は、認証済みの前記第2の通信装置の前記ID情報を認証済みID情報として記憶しておき、以降、認証要求を受けた場合、受信したID情報が前記認証済みID情報かどうか調べ、認証済みの場合には、認証済み処理手順として、前記第2の通信装置および前記第3の通信装置における前記暗号鍵の選択の有無、前記第1の認証応答および前記第1の認証応答の転送の有無、前記第2の認証応答および前記第2の認証応答の有無、および、前記暗号化されたチャレンジを復号化し、送信したチャレンジとの一致を判定する動作の有無、にかかわらず、前記第3の通信装置は、認証成功を前記第1の通信装置を経由して前記第2の通信装置に通知することを特徴とする(4)記載の認証システム。

【0022】

(14)前記第1の通信装置が複数ある場合であって、前記第1の通信装置自身が記憶する認証済みID情報の中に、認証要求を受け付けたID情報が含まれていない場合、自身以外の第1の通信装置に問い合わせ、自身以外の第1の通信装置の何れかにおいて認証済みの場合、前記認証済み処理手順を行うことを特徴とする(10)または(12)何れか記載の認証システム。

【0023】

(15)前記第1の通信装置が複数ある場合であって、各第1の通信装置は、自身で認証した認証済みID情報を他の第1の通信装置に通知して、各第1の通信装置が、全認証済みID情報を記憶するようにし、前記第1の通信装置の何れかが、前記第2の通信装置から認証要求を受け付けた場合、自身が記憶する認証済みID情報に、認証要求を受け付けたID情報が含まれている場合、前記認証済み処理手順を行うことを特徴とする(10)または(12)何れか記載の認証システム。

【0024】

(16)前記第1の通信装置が複数ある場合であって、各第1の通信装置は、自身で認証した認証済みID情報を前記第3の通信装置に通知し、前記第3の通信装置が全認証済みID情報を記憶するようにし、前記第1の通信装置の何れかが、前記第2の通信装置から認証要求を受け付けた場合、受け付けた前記ID情報を前記第3の通信装置に通知して認証済みID情報かどうか判定し、認証済みと判定された場合、前記認証済み処理手順を行うことを特徴とする(11)または(13)何れか記載の認証システム。

【0025】

(17)前記第2の通信装置に接続切断モード選択部を設け、ユーザが前記接続切断モ

ードで送られると、切断電文が前記第1の通信装置に返信され、前記ネットワーク内の装置が記憶している認証済みID情報から前記第2の通信装置のID情報を消去することを特徴とする(10)乃至(16)何れか記載の認証システム。

【0026】

(18)前記第1の通信装置、または、前記第3の通信装置に、認証済みID情報を表示できる表示部と、表示された認証済みID情報の何れかを削除する操作部を設け、前記ネットワーク内の装置が記憶している認証済みID情報から所定の前記第2の通信装置の認証を解除することができるようにしたことを特徴とする(10)乃至(16)何れか記載の認証システム。

【0027】

(19)前記第2の通信装置が複数あり、同時に認証要求できる認証システムであって、前記複数の第2の通信装置において、それぞれの前記暗号鍵選択部により前記複数の暗号鍵から同一の暗号鍵を選択することにより、前記複数の第2の通信装置が、並列して認証されることができることを特徴とする(3)乃至(4)何れか記載の認証システム。

【0028】

(20)前記表示部と前記認証入力部をリモコン装置上に設け、前記第1の通信装置と前記リモコン装置との間に通信路を設け、ユーザが手元で、認証入力を行うようにしたことを特徴とする(1)記載の認証システム。

【0029】

(21)前記表示部と前記認証入力部をリモコン装置上に設け、前記第3の通信装置と前記リモコン装置との間に通信路を設け、ユーザが手元で、認証入力を行うようにしたことを特徴とする(2)記載の認証システム。

【0030】

(22)前記暗号鍵選択部をリモコン装置上に設け、前記第1の通信装置と前記リモコン装置との間に通信路を設け、ユーザが手元で、前記暗号鍵選択部により前記複数の暗号鍵から1つを選択するようにしたことを特徴とする(3)記載の認証システム。

【0031】

(23)前記暗号鍵選択部をリモコン装置上に設け、前記第3の通信装置と前記リモコン装置との間に通信路を設け、ユーザが手元で、前記暗号鍵選択部により前記複数の暗号鍵から1つを選択するようにしたことを特徴とする(4)記載の認証システム。

【0032】

(24)上記(1)乃至(23)何れか記載の第1の通信装置または第2の通信装置または第3の通信装置。

【0033】

(25)複数の通信装置からなるネットワークにおいて、第1の通信装置が第2の通信装置の認証を行うシステムであって、前記第1の通信装置は、本体部とリモコン装置を備え、リモコン装置は、本体部と着脱可能に構成され、前記リモコン装置は、認証用の操作部及び表示部を備え、前記本体部と前記リモコン装置との間に無線通信路を設け、前記リモコン装置を前記本体部から外す際に、共有鍵を設定し、前記リモコン装置を前記本体部から外した状態において、前記共有鍵を使用して、前記操作部及び表示部に関わる情報を暗号化通信することを特徴とする認証システム。

【0034】

前記従来の課題を解決するために、本発明は、セキュリティを向上させるために、前記2つの認証モードを提供する。また、コストを削減するために、無線LAN自体の通信手段を用い、他の通信手段はなくともよい。

【0035】

(1)、(2)に記載のシステムによって、ユーザは第三者として、簡単にAPとクライアントとの相互認証をさせることができる。

【0036】

(3)、(4)に記載のシステムによって、ユーザは日常生活にあるナンバーロックの

数字を口わして鍵を開けるのと同じように、ＡＰまたはルータとクライアントとの共通秘密暗号鍵を選択することで、相互認証をさせることができる。

【００３７】

（６）に記載のシステムによって、有線通信手段も、無線通信特別設定モードも不要となり、標準の無線通信手段とモードがあれば、認証と設定を行うことができる。

【００３８】

（１０）から（１３）に記載のシステムによって、再接続の際に、認証・設定が簡単化することができる。

【００３９】

（１４）から（１６）に記載のシステムによって、クライアントは複数のＡＰが設置されているネットワーク中に移動しても、ユーザの認証なくそのまま再接続することができる。

【００４０】

（１７）、（１８）に記載のシステムによって、接続解消時の操作の簡単化及び、認証・接続に関する情報を抹消することにより、機器の譲渡や廃棄に備え、セキュリティを向上することができる。

【００４１】

（１９）に記載のシステムによって、ＡＰまたはルータと複数台のクライアントとの認証・接続を一括に行い、一台一台煩雑な設定はあまり手間がかからずにできる。

【００４２】

（２０）から（２４）に記載のシステムによって、ユーザは遠隔で認証操作することができる。

【発明の効果】

【００４３】

本発明によれば、表示部を用いての目視による認証、または共通秘密暗号鍵の使用による認証を行うことで、侵入や誤接続を防ぐことにより、セキュリティが向上できる。また、２つの認証モードのいずれもユーザにとってシンプルで実行しやすい。特に、認証モード２の実行は、通常のナンバーロックの操作と似たような感覚で操作するので、普通のユーザにとって覚えやすい。なお、認証モード２では、数字を合わせるだけで複数台のクライアントを一週に認証することもできる。

【００４４】

また、クライアントのＩＤ情報を保存することで、クライアントの再接続時に、再確認や再認証を行わずに接続の保持ができる。さらに、クライアントのＩＤ情報を複数のＡＰまたはルータの間で共有する仕組みを提供することにより、クライアントが移動する際にも、再確認や再認証を行わずに接続の保持ができる。

【００４５】

このような２つの設定モードを同時に実装することにより、設定方法を柔軟に選択することができる。ＩＥＥＥ ８０２．１１の標準に合わせることができる。

【００４６】

なお、本発明によれば、認証専用の有線インターフェイスも、無線出力パワーを下げるような特別な設定専用モードも不要となり、コスト削減が達成できる。

【００４７】

なお、本発明を有線方式のネットワークに適用することも可能であり、認証が簡単に行えるという本発明の効果が得られる。

【発明を実施するための最良の形態】

【００４８】

以下本発明の実施の形態について、図面を参照しながら説明する。まず、以下説明する各実施の形態に使用するアクセスポイント装置とクライアント装置について、全体的な構成及び各部分の機能を説明する。

【００４９】

図1には、本発明に採用するＡＰ１（ノードホスト装置）またはルータとクライアント２の各装置の基本的な構成およびそれらの装置を用いた認証システムを示す。ＡＰ１は、無線ＬＡＮカード１０、設定モード選択部１１と、表示部１２と、暗号鍵選択部１３と、暗号鍵を保存する記憶部１４とを有する。クライアント２は、無線ＬＡＮカード２０、設定モード選択部２１と、表示部２２と、暗号鍵選択部２３と、暗号鍵を保存する記憶部２４とを有する。ＡＰ１とクライアントは無線ＬＡＮで通信可能である。

【００５０】

なお、ＡＰ１とクライアント２は、サポートする認証モードにより、前記の各部の内の一部を設置しなくてもよい。例えば、後述する認証モード１のみサポートする場合には、ＡＰまたはルータは、暗号鍵選択部１３と暗号鍵を保存する記憶部１４とを設置する必要がない。また、図示しないが、ユーザが操作できる認証入力部を設ける。また、クライアント２は、認証モード１のみサポートする場合には、表示部２２と、暗号鍵選択部２３と、暗号鍵を保存する記憶部２４とを設置する必要がない。

【００５１】

設定モード選択部１１と２１は、１つまたは複数の認証モード及び通信切断モードを選択するために設けられる。従って、認証モードを１つだけサポートする場合は少なくとも２つの選択ができ、２つの認証モードをサポートする場合は少なくとも３つの選択ができるようにする。設定モード選択部に手動設定モードを設けることも可能である。また、自動的にモードを選択するようにすることも可能である。

【００５２】

表示部１２は、ユーザの目視認証の際に用いられる。クライアントから接続要求があるとき、クライアントを特定できる情報（例えば、名前またはＭＡＣアドレス）が表示部に表示され、ユーザはそれを見て確認し、接続の許可・不許可の判断を行う。表示部で表示する情報は名前またはＭＡＣアドレスに限られない。表示部は液晶が手軽であるが、他の表示デバイスでもよい。

【００５３】

後述する認証モード２において、暗号鍵選択部１３と２３は、記憶部に保存されている暗号鍵を選択する際に用いられる。暗号鍵選択部は普通ジョグダイヤルなどのダイヤル式の機構部を採用するが、ほかの機構、例えば、数字ボタンを並べたものでもよい。暗号鍵選択部１３、２３の選択値は前記表示部１２、１３に表示され、ユーザは目視確認ができるようにする。０００から９９９までの暗号鍵番号を１０００種類の暗号鍵符号に割り当て、ジョグダイヤルを使用して暗号鍵番号を選択し、選択した暗号鍵番号を表示部１２、２２に表示するようすれば、十分に多種類の暗号鍵を用意することができ、その選択も簡単である。選択値としては、暗号鍵番号の代りに、別の暗号鍵識別子、たとえば、アルファベットを用いてもよい。

【００５４】

記憶部１４と２４は、秘密暗号鍵の保存に用いられる。順番は、ＡＰ１とクライアント２で統一されており、同じ暗号鍵番号の暗号鍵符号は必ず同じである。記憶部は、無線ＬＡＮカードに組み込まれている非揮発性メモリを用いてもよいし、メモリカードを用いるようにしてもよい。

【００５５】

上記無線ＬＡＮカード１０、２０は、互いに所定の無線ＬＡＮ規格のプロトコルに従って通信を行う。また、所定の無線ＬＡＮ規格のプロトコルに従って、後述する各種電文の生成と送信、電文の受信と解析を行い、更に、電文に搭載する情報の生成、暗号化、受信した情報の復号化、記憶処理などの処理を行う。無線ＬＡＮカード１０、２０は、無線ＬＡＮプロトコル処理部と呼んでもよい。

【００５６】

次に、上記ＡＰ１とクライアント２が行う認証の手順について説明する。以下の説明において、特に断らない場合、同じ電文の手順には同じ番号を付し、再度の説明を省く場合がある。

（実施の形態１）

上記説明した構成を有するＡＰ１とクライアント２の間において行う本発明の認証システムでの認証方法のうち、認証モード１の方法について説明する。認証モード１は、ユーザだけが知っている、クライアント装置毎に割り振られたＩＤをユーザ自身が目視で認証する点に特徴がある。認証モード１の実施にあたっては、まず、設定モード選択部で認証モード１を選択する。ＡＰまたはルータとクライアント両方において同じ認証モード１を選択する。なお、認証モードとして認証モード１のみの場合は、認証モードの選択手順を省いてもよい。認証は、ＡＰまたはルータとクライアントとの間で行われる。認証モード１の実施は、従来ＩＥＥＥ ８０２．１１のオープン認証方式の流れと相似する。また、ＡＰ１とクライアント２においてやり取りする電文の形式は、ＩＥＥＥ ８０２．１１の無線ＬＡＮのＭＡＣレイヤ規格に従ったものでよく、公知の電文形式が利用できるので電文形式の詳細の説明を省く。なお、ＩＥＥＥ ８０２．１１の無線ＬＡＮのＭＡＣレイヤ規格以外のプロトコルであってもよいことはいうまでもない。以下に、図を参照しながら本発明の実施に直接関わる部分について詳細に説明する。

【００５８】

図２において、クライアント２とＡＰ１との間においてまずプローブ要求１００、プローブ応答１０１の送信を行う。この通信によりクライアント２の近傍にＡＰ１が存在することが確認される。次に、ＡＰ１はクライアント２からクライアント２のＩＤ情報（アイデンティティ情報、例えば、名前またはＭＡＣアドレス）を含む認証要求（ＩＤ）１０２を受信し、そのＩＤ情報をＡＰ１の表示部１２に表示する。ユーザは、表示されたＩＤを見て、正しいＩＤ情報であるかを確認し、正しいと判断した場合、認証入力部（例えば、専用ボタンまたは暗号鍵選択部または暗号鍵選択部に設けられた認証許可と不許可を入力するボタン、スイッチなど）を操作することにより、認証を許可する。ＡＰ１は、ユーザの認証許可指示を得て、クライアントへ認証成功１０４を送信する。認証成功１０４を受信したクライアント２は、ＡＰ１へアソシエーション要求１０５を送信し、ＡＰ１はクライアント２へアソシエーション応答１０６を返信する。以上で、接続認証が終わる。次に、接続設定を行う。

【００５９】

表示部１２に、ユーザの知らないＩＤが表示された場合や、予め予想しないＩＤが表示された場合には、ユーザは認証を不許可とすることができる。図３は、ユーザは認証要求（ＩＤ）１０２に対して、認証入力部の操作により、認証の不許可を出す場合のシーケンスである。電文１０４において、認証失敗をクライアント２に通知する。指定時間内にユーザからの返事がない、すなわち、タイムアウトの場合には、クライアント２は認証不許可と同じように見なす。図２に於けるアソシエーション要求以降のアクションを行わない。

【００６０】

なお、上記ＩＤ情報は、予めクライアント２に割り振られているものでもよいが、クライアント２にＩＤ情報入力部を設けて、ユーザが自身の宅内で独自に決めたＩＤ情報体系に従って、ＩＤ情報を入力するのが好ましい。このＩＤ情報入力の仕組みは、専用のボタン・スイッチ、テンキー、タッチパネル、リモコンによる入力、ＰＤＡや携帯電話の操作部を利用した入力など、種々の方式を適用できる。

【００６１】

なお、本実施の形態において、上記ＡＰ１を第１の通信装置とし、クライアント２を前記第２の通信装置と呼べば、第１の通信装置が第２の通信装置の認証を行うシステムとみなすことができる。

【００６２】

（実施の形態２）

図４のシーケンスはＩＥＥＥ ８０２．１１の新しい認証モデルに沿ったもので、認証処理は、クライアント２とＡＰ１とのアソシエーションが確立された後に、ＡＰ１から起

動される。認証の方法は、上記実施の形態１と同様の認証モード１に属し、ユーザによる目視認証を利用する。アソシエーション要求４０４とその応答４０５の手順が成功すると、ＡＰ１は認証者として、クライアント２へＥＡＰプロトコルに基づいてＥＡＰ ＩＤ要求４０６を送信する。クライアント２は、自分のＩＤ情報（例えば、名前またはＭＡＣアドレス）を含んだＥＡＰ ＩＤ応答４０７を返信する。ＡＰ１は、そのＩＤ情報を自分の表示部に表示する。ユーザはそれを確認し、認証を許可する。これを受けてＡＰ１は、認証成功４０９をクライアント２へ送信する。ちなみに、ＩＥＥＥ ８０２．１１の新しい認証モデルでは、この図の中の認証要求４０２と認証応答４０３では、実質的な認証を行わないことになっている。

【００６３】

図５は、ユーザは不許可を出した場合、または指定時間内に認証入力部を操作せず、不返答となったときのケースである。この場合、ＡＰ１からクライアント２へ認証失敗４０９が送られる。図４、図５におけるユーザの目視認証４０８は、図２、図３におけるユーザの目視認証１０３と、それぞれ同じ動作である。

【００６４】

なお、本実施の形態において、上記ＡＰ１を第１の通信装置とし、クライアント２を前記第２の通信装置と呼べば、第１の通信装置が第２の通信装置の認証を行うシステムとみなすことができる。

【００６５】

（実施の形態３）

図６は、ユーザによる認証を各ＡＰではなく、ルータで行う場合のシーケンスを示すものである。認証の方法は、上記実施の形態１と同様の認証モード１、すなわち、ユーザによる目視認証による。ルータ３は、図２～図５におけるＡＰ１と同様の機能に加えて、ＡＰ４との間で有線または無線通信を行う機能を備える。ＡＰ４は、ルータ３との間で有線または無線通信が行う機能を備えるが、設定モード選択部１１、表示部１２、暗号鍵選択部１３はなくともよい。代りに、ＡＰ４は、図１、図２におけるＡＰ１が行った認証に関する処理をルータ３に依頼する。ＡＰ４は、クライアント１からの認証要求（ＩＤ）６０２を受信すると、電文６０３として、直ちにルータ３へ転送する。ユーザは、ルータ３の表示部に表示されているクライアント２のＩＤ情報（例えば、名前またはＭＡＣアドレス）を見て、許可か不許可の判断と認証入力操作を行う。ルータ３は、ユーザが認証を許可した場合にはルータから認証成功の応答を、不許可とした（指定時間内不返答を含む）場合には、認証失敗の応答を、それぞれ電文６０５としてＡＰ４に送る。ＡＰ４は、電文６０５を受け取ると、電文６０６としてクライアント２へ転送する。かつ、ＡＰ４は、クライアント２を認証許可したことをＡＰ４内部に記憶し、この後のアソシエーション処理や通信接続処理を行うことを可能にする。そのうえで、認証成功した場合は、以降、ＡＰ４とクライアント２の間で、アソシエーション要求６０７以降のメッセージの送受信を行う。その他の電文については、図２、図３における電文と同様である。

【００６６】

本実施の形態によれば、各ＡＰには認証の機能を備える必要が無く、ルータに集中的に認証機能を備えればよいので、ＡＰの構成が簡単になる。

【００６７】

なお、本実施の形態において、上記ＡＰ４を第１の通信装置とし、クライアント２を前記第２の通信装置とし、ルータ３を第３の通信装置と呼べば、第３の通信装置が第２の通信装置の認証を行うシステムとみなすことができる。

【００６８】

（実施の形態４）

図７は、上記実施の形態２と同様に、ＩＥＥＥ ８０２．１１の新しい認証モデルの手順に沿ったシーケンスによるものである。認証は、ＡＰ１とクライアント２との間でアソシエーションが確立された後に行われる。認証の方法は、上記実施の形態３と同様の認証モード１に属し、ユーザによる目視認証による。図４の場合と同様に、ＡＰ４側から

にＡＰ１は、電文７０７を受信したＡＰ１は、直ちに電文７０８としてルータ３へ転送する。ＥＡＰ ＩＤ 応答７０８に含まれているＩＤ情報（例えば、名前またはＭＡＣアドレス）がルータ３の表示部に表示され、ユーザはそれを見て確認し、許可か不許可（指定時間内不返答を含む）の操作を行う。それに対応する認証応答７１０はＡＰ１へ返信され、ＡＰ１は、電文７１０を受け取った後、認証応答７１１をクライアントへ転送する。その他の電文送受信の手順は、図４、図５の実施の形態２と同様である。

【００６９】

本実施の形態によれば、各ＡＰには認証の機能を備える必要が無く、ルータに集中的に認証機能を備えればよいので、ＡＰの構成が簡単になる。

【００７０】

なお、本実施の形態において、上記ＡＰ４を第１の通信装置とし、クライアント２を前記第２の通信装置とし、ルータ３を第３の通信装置と呼べば、第３の通信装置が第２の通信装置の認証を行うシステムとみなすことができる。

【００７１】

（実施の形態５）

次に暗号鍵を使用する本発明の認証モード２の手順について説明する。認証モード２においては、本発明の認証システムを構成するＡＰ１とクライアント２において、図１で説明した、設定モード選択部１１、２１、表示部１２、２２、暗号鍵選択部１３、２３、記憶部１４、２４をそれぞれ備えるものとする。認証モード２の実施にあたっては、まず、ＡＰとクライアント両方において同じ認証モード２を選択する。それから、暗号鍵選択部を操作してＡＰとクライアントにおいて同じ暗号鍵を選択する。以下に、図を参照しながら実施における詳細な手順を説明する。

【００７２】

図８において、ＡＰ１とクライアント２の両方で、設定モード選択部１１と２１を操作して認証モード２を選択する。次に、暗号鍵選択部１３と２３を操作してＡＰ１とクライアント２において同じ暗号鍵を選択する。なお、認証モードの選択と暗号鍵の選択は順序が逆でもよい。また、ＡＰ１において、設定モード選択部１１と暗号鍵選択部１３の選択を同時に行ってもよい。また、クライアント２においても、設定モード選択部２１と暗号鍵選択部２３の選択を同時に行ってもよい。暗号鍵の選択は、ジョグダイヤルなどの操作により、暗号鍵番号や暗号鍵識別子を選択して行う。ユーザが暗号鍵の選択動作を行うと、ＡＰ１は暗号鍵選択部の選択値を読み取り、記憶部に保存されている対応する暗号鍵を読み出し、この暗号鍵をその後の認証に使用する。クライアント２でも同じことを行う。ＡＰ１とクライアントとの間で、プロンプトメッセージ８０２、８０３の交換を終えると、クライアント２は、認証要求８０４をＡＰ１へ送信する。電文８０４を受信したＡＰ１は、乱数を生成し、この乱数をノンスとして、チャレンジを伴う認証応答８０５にのせて、クライアント２に送信する。クライアント２は、先に選択された暗号鍵を用いて受信したノンスを暗号化し、暗号化済みチャレンジとして認証応答８０６にのせてＡＰ１へ返信する。ＡＰ１は、受信した暗号化済みノンスを、先に選択された暗号鍵で復号化して、その結果を先に送った暗号化前のノンスと比較する。ＡＰ１は、２つのノンスが一致すれば認証応答（成功）を、一致しなければ認証応答（失敗）を、認証応答電文８０７としてクライアント２へ送信する。その後のアソシエーションなどの手順は、前記実施の形態１や実施の形態３の場合と同じなので、説明を省略する。

【００７３】

認証モード２を１種類だけ備えている場合は、認証モード選択の手順はなくともよいし、設定モード選択部を省いてもよい。

【００７４】

本実施の形態では、クライアント２を識別するＩＤ情報は、認証のためにはあってもなくてもよい。しかしながら、クライアント２が複数ある場合は、通信相手として区別する必要があるので、一般的には、ＩＤ情報も伝送される。

【 0 0 7 5 】

なお、本実施の形態において、上記 A P 1 を第 1 の通信装置とし、クライアント 2 を前記第 2 の通信装置と呼べば、第 1 の通信装置が第 2 の通信装置の認証を行うシステムとみなすことができる。

【 0 0 7 6 】

(実施の形態 6)

認証モード 2 の場合も、図 6 において説明した実施の形態 3 と同様に、A P の代りにルータ 3 が認証を行うシステムの形態を適用できる。図 9 は、認証を、A P 1 ではなく、ルータ 3 で行うようにした実施の形態である。ルータ 3 は、図 1 に示した A P 1 と同様に、設定モード選択部 1 1、表示部 1 2、暗号鍵選択部 1 3、記憶部 1 4 を備え、更に A P 4 との間で無線通信、または有線通信を行う機能を有する。A P 4 は、設定モード選択部 1 1、表示部 1 2、暗号鍵選択部 1 3、記憶部 1 4 がなくともよく、ルータ 3 と無線通信、または有線通信を行う機能を有し、クライアント 2 との間で無線 LAN による通信を行う機能を有する。A P 4 は、クライアント 2 から認証要求 9 0 4 を受信した後、直ちにルータ 3 へ電文 9 0 5 により転送する。認証に関するメッセージのやりとりは、A P 4 を介して、ルータ 3 とクライアント 2 との間で行われる。A P 4 は、転送の役割を果たしながら、その後のクライアント 2 との接続のために、認証の結果を捕捉認識して記憶する。

【 0 0 7 7 】

一回認証されたクライアントの I D は、クライアントから永久切断要求がない限りずっと、認証した A P またはルータに保存される。こうすることにより、一時切断してまた再接続の要求を出したクライアントに対しては、このクライアントの I D を認証済みの I D として既に持っているため、再度の認証の手続きが不要となる。

【 0 0 7 8 】

なお、本実施の形態において、上記 A P 4 を第 1 の通信装置とし、クライアント 2 を前記第 2 の通信装置とし、ルータ 3 を第 3 の通信装置と呼べば、第 3 の通信装置が第 2 の通信装置の認証を行うシステムとみなすことができる。

【 0 0 7 9 】

(実施の形態 7)

また、ネットワーク内に複数の A P が存在する場合、クライアントが 1 つの A P から他の A P 近くまで移動した場合、新たな A P との間で再接続を行う必要がでてくる。この再接続においては、あらためて認証を行うか、または、行わないか、の 2 つの実施の形態が考えられる。認証をあらためて行う形態では、上記各実施の形態の何れかの手順を実行して新規にクライアント 2 の認証が行われるので、複数の A P の間で認証済みのクライアントに関する情報交換をしておく必要がない。これに対して、認証をあらためて行わない形態では、前の認証を再利用する必要がある、A P の間でクライアントの認証結果に関する情報交換をする必要がある。過去の認証を再利用する場合、過去の認証情報を何処に保存するか、どのように再利用するかによって、いくつかの実施の形態が考えられる。以下には、それらの実施の形態について順に説明する。

【 0 0 8 0 】

まず、クライアントの I D 情報の共有の 3 つの方式について述べる。第 1 の方式：A P 共有方式 (A) は、認証したクライアントの全 I D 情報を全 A P の間で共有する方式である。第 2 の方式：A P 分散管理方式 (B) は、A P が自身で認証したクライアントの I D 情報のみを自身で管理し、A P 全体でクライアントの全 I D を分散的に共有する方式である。第 3 の方式：ルータ共有方式 (C) は、認証済みのクライアントの全 I D 情報をルータに保存共有するタイプである。

【 0 0 8 1 】

A P 共有方式 (A) に用いられるクライアントの I D 情報の共有の仕組みについて、図 1 0 と図 1 1 を用いて説明する。図 1 0 において、認証応答 (成功) 1 0 0 0 で示すように、A P 1 においてクライアント 2 に対する認証が成功すると、A P 1 は、認証済みのクライアント 2 の I D をのせたクライアントアナウンス 1 0 0 1 を、ネットワーク内の全 A

図 15、図 16、図 17 を用いて説明する。

【0087】

クライアントをネットワークから永久に切り離すには、図 15 のように、手順 1501 のように、クライアント 2 の設定モード選択部を切断モードに切り替えて、クライアント 2 から AP 1 へ自身の ID を付けて切断電文 1502 を送る。切断電文を受信した AP 1 は、クライアント 2 の ID 情報を、手順 1503 により、自分のデータベースから削除する。このためには、第 2 の通信装置であるクライアント 2 の設定モード選択部に接続切断モードスイッチなどの接続切断モード選択部を設け、ユーザが前記接続切断モードを選択すると、切断電文が第 1 の通信装置である AP 1 に送信され、前記ネットワーク内の装置が記憶している認証済み ID 情報から第 2 の通信装置の ID 情報を消去するようにすればよい。

【0088】

AP 1 以外に他の AP が認証済み ID 情報を共有する前記実施の形態 7 の AP 共有方式 (A) や AP 分散管理方式 (B) のような方式の場合には、図 16 に示すように、切断電文 1602 を受信した AP 1 は、マルチキャストの切断電文 1603 により、消去すべき認証済み ID 情報を AP a5 に通知して消去を要求し、消去要求を受信した AP a は、前記消去すべき認証済み ID 情報を記憶している場合、その ID 情報を消去する。最初に切断電文を受信した AP 1 でも、認証済み ID 情報にクライアント 2 の ID 情報を記憶している場合、手順 1604 において、消去する。AP a5 は、認証済み ID 情報を消去ののち、切断応答電文 1606 を AP 1 に返す。その後、AP 1 は、切断応答電文 1607 をクライアント 2 に返す。

【0089】

認証済み ID 情報をルータ 3 が保存するルータ共有方式 (C) では、図 17 のようにする。図 17 において、クライアント 2 が設定モード選択部を切断モードに切り替えると、クライアント 2 は最寄の AP 4 に切断電文 1702 に自身の ID 情報を付加して送信する。AP 4 は、切断電文 1702 を切断電文 1703 として、ルータ 3 に転送する。ルータ 3 は、受信した ID 情報が認証済み ID 情報かどうか確認し、認証済みの場合、手順 1704 において、その ID 情報を消去する。その後、切断応答 1705 を AP 4 に返信し、AP 4 は、切断応答 1706 として、クライアント 2 に転送する。

【0090】

また、クライアントに対して前記の切断処理をしないまま、電源を切断するなどして永久に切り離した場合には、ユーザは、AP またはルータに備えられている、そのクライアントの ID を直接削除する機能を利用するようにしてもよい。このためには、第 1 の通信装置である AP 1、または、第 3 の通信装置であるルータ 3 に、認証済み ID 情報を表示できる表示部と、表示された認証済み ID 情報の何れかを削除する操作部を設け、ネットワーク内の装置が記憶している認証済み ID 情報から所定または所望の第 2 の通信装置であるクライアントの認証を解除することができるようにすればよい。認証済み ID 情報を複数のアドレスポイントに記憶する方式の場合は、マルチキャストの消去要求電文により、消去すべき認証済み ID 情報を通知し、消去要求を受信した AP やルータは、前記消去すべき認証済み ID 情報を記憶している場合、消去するようにすればよい。

【0091】

(実施の形態 9)

上記認証モード 2 の方式において、第 2 の通信装置であるクライアント 2 が複数ある場合、個々に認証作業を行うことなく、同時並行的に認証を行うことができる。複数の第 2 の通信装置において、暗号鍵選択部を操作して、それぞれの暗号鍵選択部により複数の暗号鍵から同一の暗号鍵を選択しておき、認証側の AP 1 またはルータ 3 において同一の暗号鍵を選択しておけば、前記複数の第 2 の通信装置が、並列して認証の手順が進められ、同時並行的に認証されることになる。

【0092】

(実施の形態 10)

上記実施の形態において、Ａ１が認証を行う場合、Ａ１がセグメント内に複数設置していると、ユーザはＡＰを設置してある場所へ移動する必要がある。認証モード１の場合、ＡＰの表示部の情報を表示部付の手元リモコン装置により見ることができるようになれば、移動が不必要になる。リモコンとＡＰの間でセキュアな無線通信路を設定できるようにすればよい。リモコンはＩＤ情報を確認し、認証許可を指示するための機能でよいので、暗号化などのない簡単な伝送路を適用してもよい。

【００９３】

このためには、認証モード１の場合、前記第１の通信装置であるＡＰ１の前記表示部と前記認証入力部をリモコン装置上に設け、ＡＰ１の本体と前記リモコン装置との間に通信路を設け、ユーザが手元で、認証入力を行うようにすればよい。前記第３の通信装置であるルータ３が認証を行うシステムの場合も、同様のリモコン構成とすれば、同様の作業を行うことができる。

【００９４】

認証モード２の場合、前記第１の通信装置であるＡＰ１の前記暗号選択部をリモコン装置上に設け、ＡＰ１の本体と前記リモコン装置との間に通信路を設け、ユーザが手元で、前記暗号鍵選択部により前記複数の暗号鍵から１つを選択するようにすればよい。前記第３の通信装置であるルータ３が認証を行うシステムの場合も、同様のリモコン構成とすれば、同様の作業を行うことができる。なお、表示部が設けられる場合は、その表示部をリモコン装置上に設けることはいうまでもない。

【００９５】

リモコン装置をＡＰ１やルータ３の本体部に設けた接続部に挿入しておく、リモコン装置と本体部分が直接結合できるようにしておき、認証処理を行う場合に、リモコン装置を本体部から取り出して、ユーザが移動できるようにしてもよい。リモコン装置を本体部からはずすときに、本体部とリモコン装置の間でリモコン無線通信用の共有鍵Ｒを決めて、以降の認証処理中に行う表示用のＩＤ情報の送信、認証許可の入力操作情報の送信、暗号鍵選択のための暗号鍵番号の送信などの本体部とリモコン装置間の通信において、共有鍵Ｒを使用して送信データを暗号化、復号化すれば、第三者に送信データの内容を知ることがなくなる。共有鍵Ｒは、リモコン装置を本体部から外すたびに新たに決めるようにすることができ、セキュアな通信路となる。

【００９６】

リモコン装置を本体部から外すときに共有鍵Ｒを設定する方法は、種々考えられる。一例として、リモコン装置を本体部から外す際に、リモコン装置の移動を検知するスイッチを本体部に設けておき、スイッチが移動を検知すると、すぐさま新たな共有鍵Ｒを本体部がリモコン装置に供給するようにすればよい。リモコン装置を本体部に挿入してある状態で、定期的に共有鍵Ｒの値を変更するようにして、リモコン装置を外したときに、最新の共有鍵Ｒを使用できるようにしてもよい。共有鍵Ｒの変更は、リモコン装置と本体部とが有線接続状態で行えるので、共有鍵を盗まれる恐れは実質上ないといえる。

【００９７】

リモコン装置をユーザが放置する、あるいは、紛失する懸念があるので、一定時間以上リモコン装置が本体部からはずされている場合、本体部とリモコン装置の何れかまたは両方が警告音を発生するようにするとよい。認証作業ののちリモコン装置を本体部に再び挿入するまで、クライアント２の通信アプリケーションを開始できないようにしてもよい。

【００９８】

（その他の実施の形態及び補足）

上記各実施の形態においては、認証される第２の通信装置がクライアント装置であるものとして説明したが、クライアント２以外の装置、例えば、ネットワーク内のリピータ装置を第２の通信装置とし、これを第１の通信装置が認証する場合にも、本発明の認証方法を使用したシステムを構成できる。リピータ装置を、アクセスポイント装置を経由して、第３の通信装置であるルータ装置が認証するネットワークに本発明を適用することもできる。すなわち、認証の必要な第２の通信装置と、認証を行う第１または第３の通信装置が

てれておけるものが向わり、半透明の認証シールドを形成することができ、両半は認証方法を実現できる。

【0099】

本発明の認証方法では、宅内ネットワークに適用する場合、AP1またはルータ3とクライアント2の傍らにユーザとその家族がそれぞれ位置することにより、声を掛け合いながら上記の認証手順を進めることができる。家族であるので、不正な認証が起きる懸念がない。ユーザが1人で認証設定する場合は、AP1またはルータ3とクライアント2と、それぞれの装置の傍にユーザが移動する必要があるが、宅内であるのでユーザの負担は小さい。

【0100】

認証モード2では、AP1またはルータ3とクライアント2において設定モード選択部や暗号鍵選択部を操作する必要があるので、それぞれの装置の傍にユーザと家族が位置するか、ユーザ本人が移動する必要があるが、宅内であるのでユーザの負担は小さい。

【0101】

上記実施の形態9のように、操作や目視を行う部分をリモコン装置のようにすれば、上記課題も解決可能である。

【0102】

認証モード1では、クライアント2のIDをユーザが目視するものである。クライアント2やAP1の送信電文が、隣家のAPやクライアント装置に受信されてしまうことが起きないとは限らないが、隣家の家人が隣家のAPやクライアント装置を同時に操作していることは稀であり、ユーザがいつ認証を行うかは隣家にはわからないので、認証内容を盗まれたり、隣家から誤った認証が侵入する恐れは少ない。これは、APやクライアント装置が、自動で認証処理を行わないことによって得られる利点である。また、ユーザが任意に決めるクライアント2のID体系が、隣家のID体系と一致することも稀である。

【0103】

上記、無線LANカード10、20は、無線LAN規格についてOSI階層モデルの各処理層の少なくとも比較的下位の層の処理を行う通信制御用のコンピュータを内蔵するものでよい。LANカードに限らず、他の形態のものでもよいことはいうまでもない。専用のコンピュータシステムでもよい。

【0104】

認証を行う前記第1の通信装置であるAP1や前記第3の通信装置であるルータ3と標準的なパソコンとの間で、セキュアな通信を有線または無線で行えるようにしておき、パソコン上に上記表示部のID情報や暗号鍵番号のような表示情報を表示し、パソコン上の画面に上記認証入力部、設定モード選択部、暗号鍵選択部などの操作部の図形を表示し、ユーザがこの表示や操作部を使用して認証処理を行うようにしてもよい。

【0105】

クライアント2を認証するためのID情報は、クライアント装置ごとに設けてもよいし、ユーザの宅内で決めた認証専用のパスワードのようなユーザ宅内の共通のIDを使用してもよい。複数のクライアント装置を使用する場合は、クライアント装置識別用のID情報と上記共通のパスワードIDを併用することになる。

【産業上の利用可能性】

【0106】

本発明は、宅内無線LAN方式のネットワークに限らず、種々のネットワークの認証システムとして活用可能性がある。

【図面の簡単な説明】

【0107】

【図1】本発明のシステム構成を示す図

【図2】本発明の認証モード1の実施の形態1におけるシーケンス図（認証成功の場合）

【図3】本発明の認証モード1の実施の形態1におけるシーケンス図（認証失敗の場合）

ロノ

【図 4】本発明の認証モード 1 の実施の形態 2 におけるシーケンス図（認証成功の場合）

【図 5】本発明の認証モード 1 の実施の形態 2 におけるシーケンス図（認証失敗の場合）

【図 6】本発明の認証モード 1 の実施の形態 3 におけるシーケンス図

【図 7】本発明の認証モード 1 の実施の形態 4 におけるシーケンス図

【図 8】本発明の認証モード 2 の認証動作のシーケンス図

【図 9】本発明の認証モード 2 の別の認証動作のシーケンス図

【図 10】本発明において A P 間のクライアントの I D 情報共有の動作手順を示すシーケンス図

【図 11】クライアントの I D 情報共有の場合の A P とクライアントとの認証動作を示すシーケンス図

【図 12】本発明において A P 間のクライアントの I D 情報共有の場合の認証動作のシーケンス図

【図 13】本発明においてクライアントの I D 情報をルータで共有する実施の形態を示すシーケンス図

【図 14】本発明においてクライアントの I D 情報をルータで共有する実施の形態の場合の認証動作を示すシーケンス図

【図 15】本発明において接続切断によりクライアントの認証済み I D 情報を消去する動作を示すシーケンス図

【図 16】本発明において接続切断により複数の A P 上のクライアント認証済み I D 情報を消去する動作を示すシーケンス図

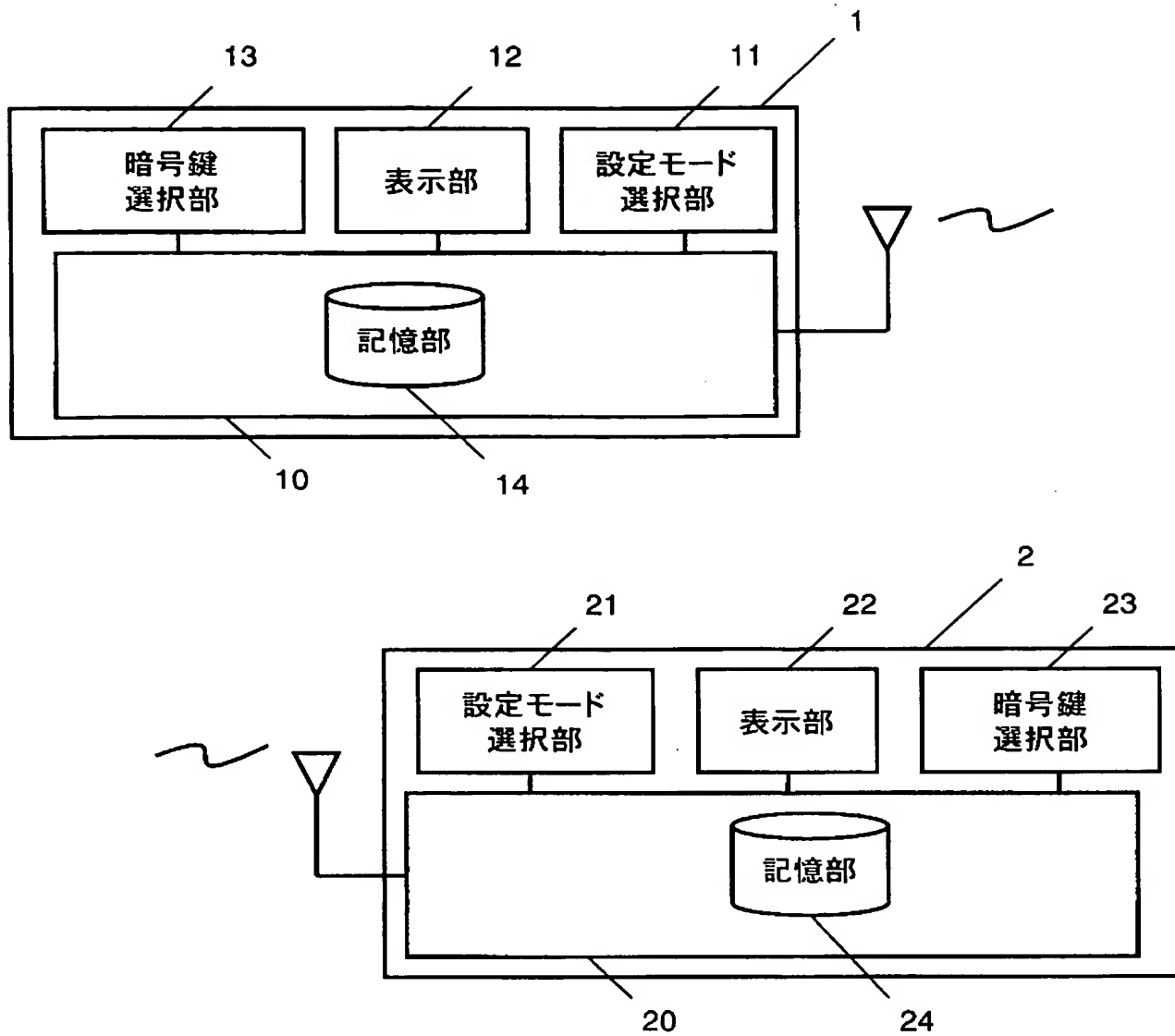
【図 17】本発明において接続切断によりルータ上のクライアント認証済み I D 情報を消去する動作を示すシーケンス図

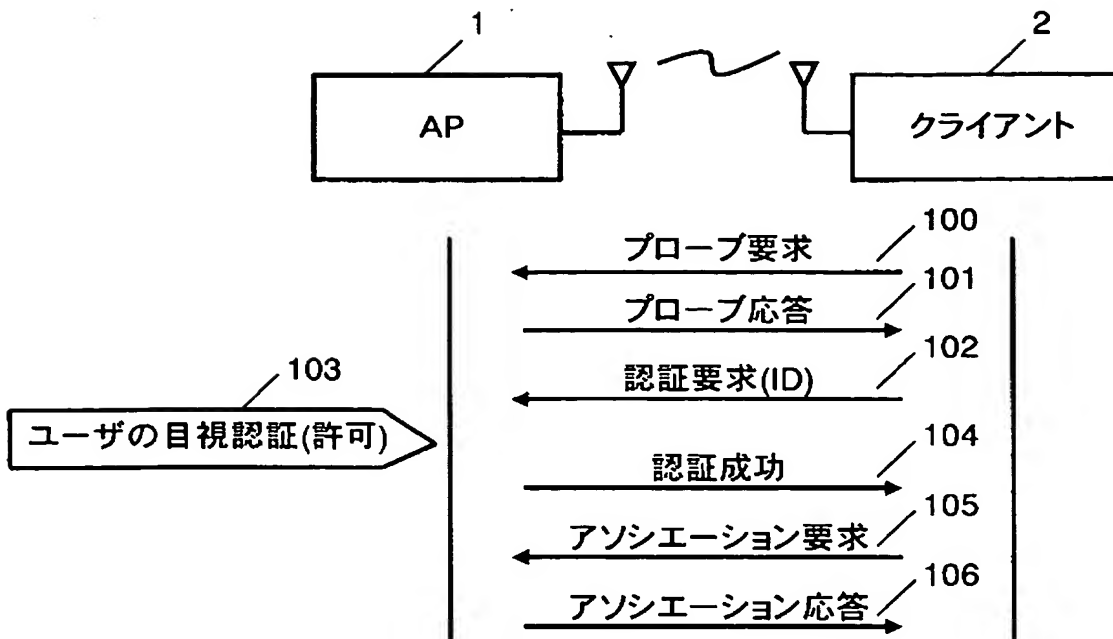
【符号の説明】

【0108】

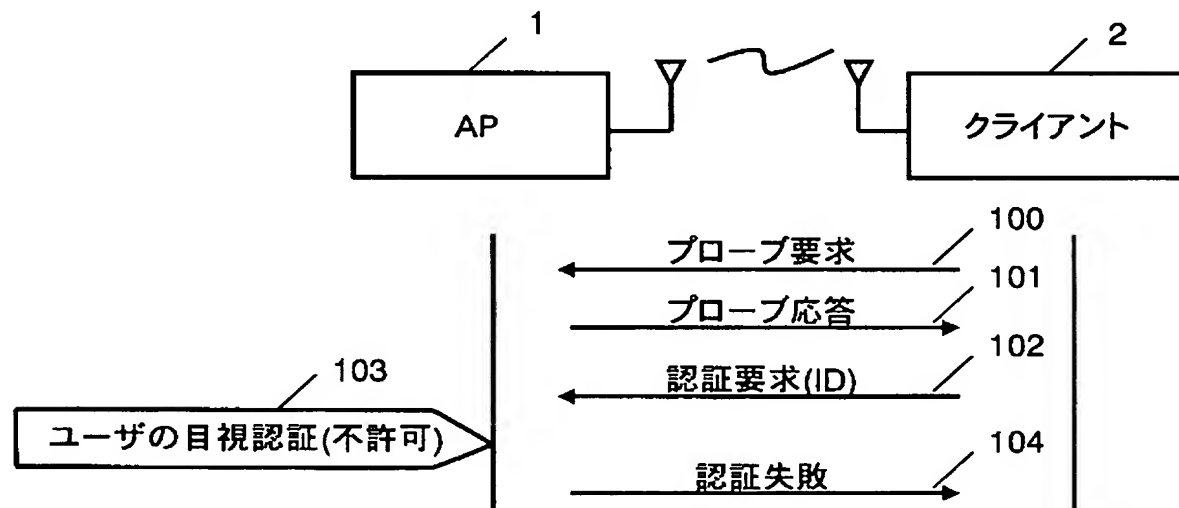
- 1 A P
- 2 クライアント
- 3 ルータ
- 10 A P またはルータの無線 L A N カード
- 11 設定モード選択部
- 12 表示部
- 13 暗号鍵選択部
- 14 記憶部
- 20 クライアントの無線 L A N カード
- 21 設定モード選択部
- 22 表示部
- 23 暗号鍵選択部
- 24 記憶部

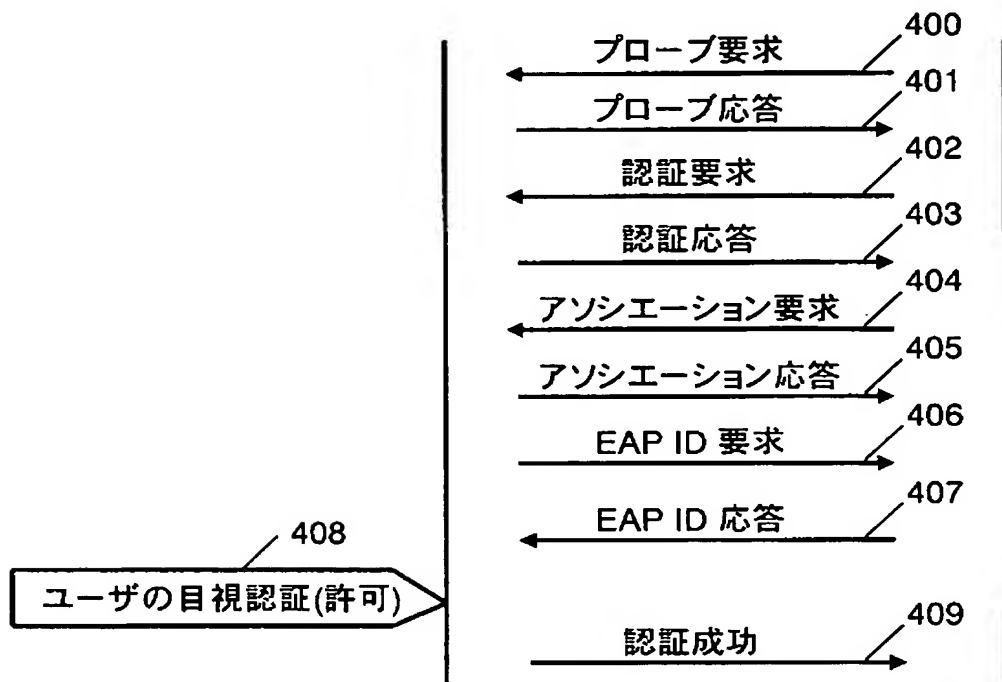
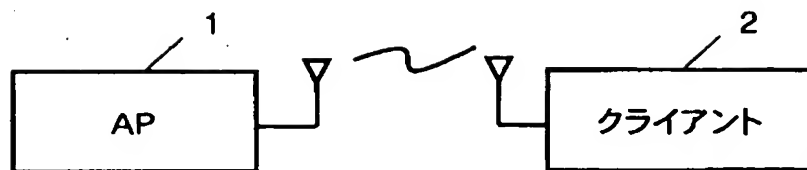
【図 1】

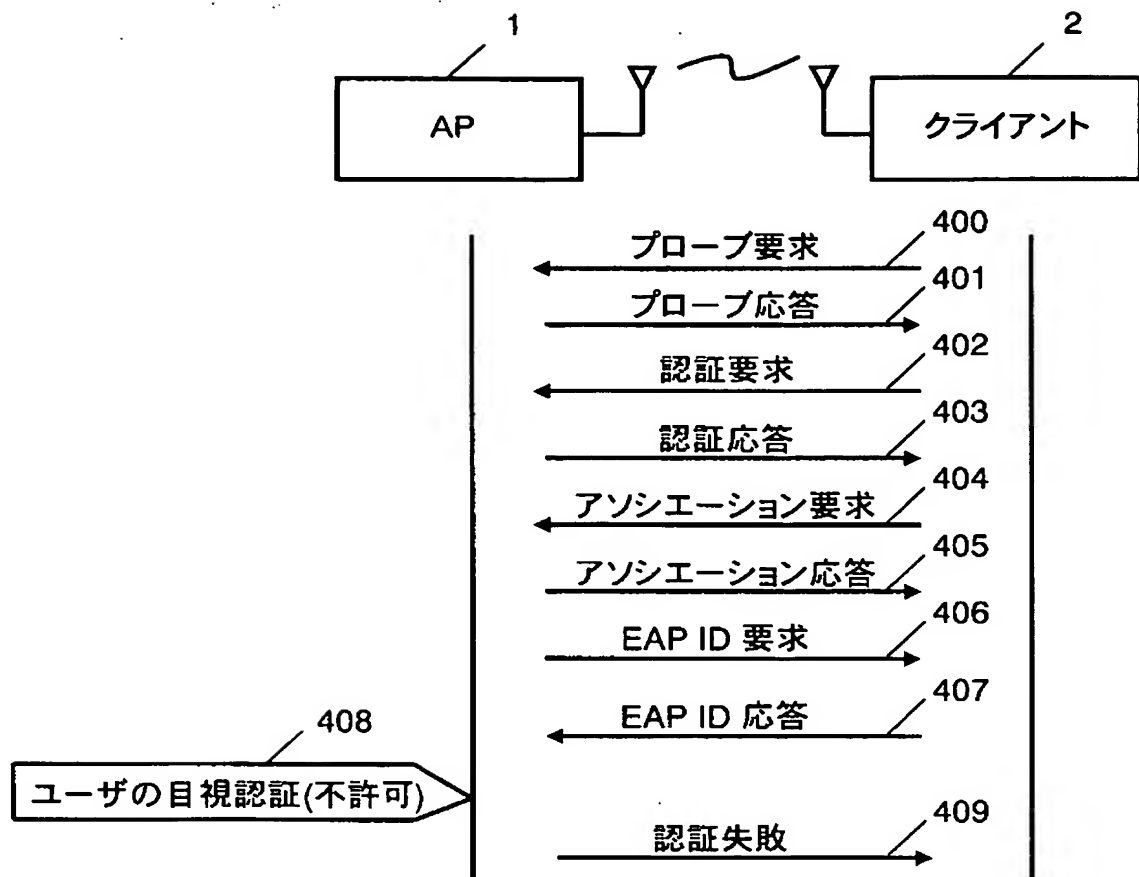




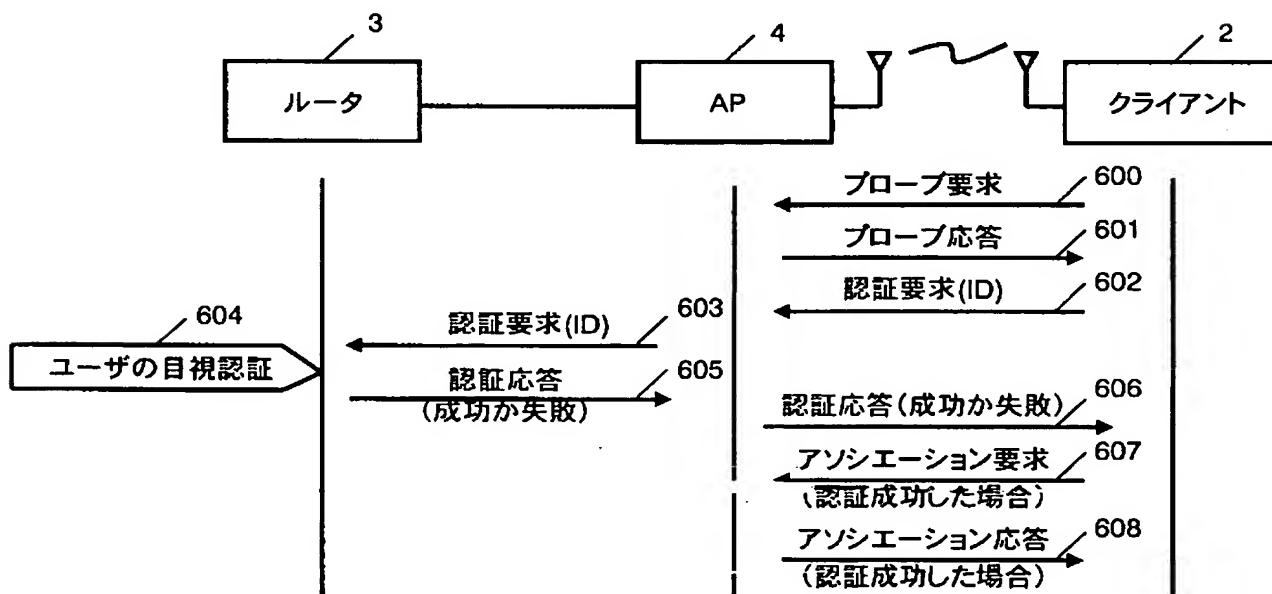
【図3】

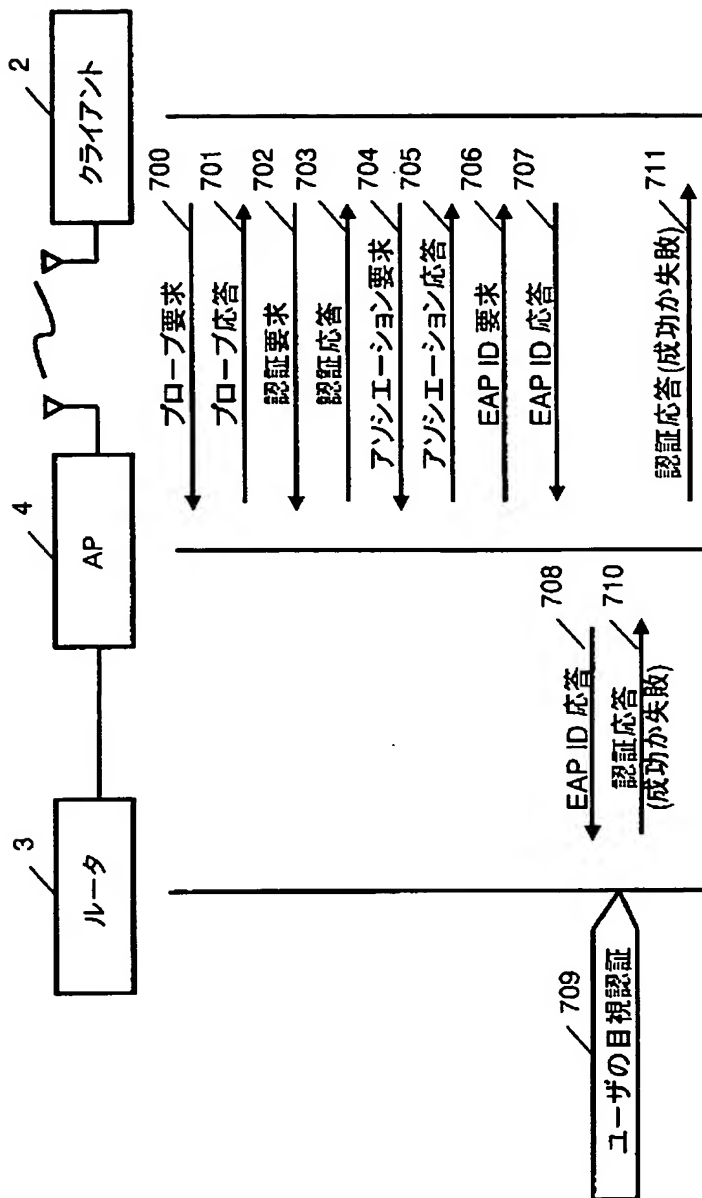


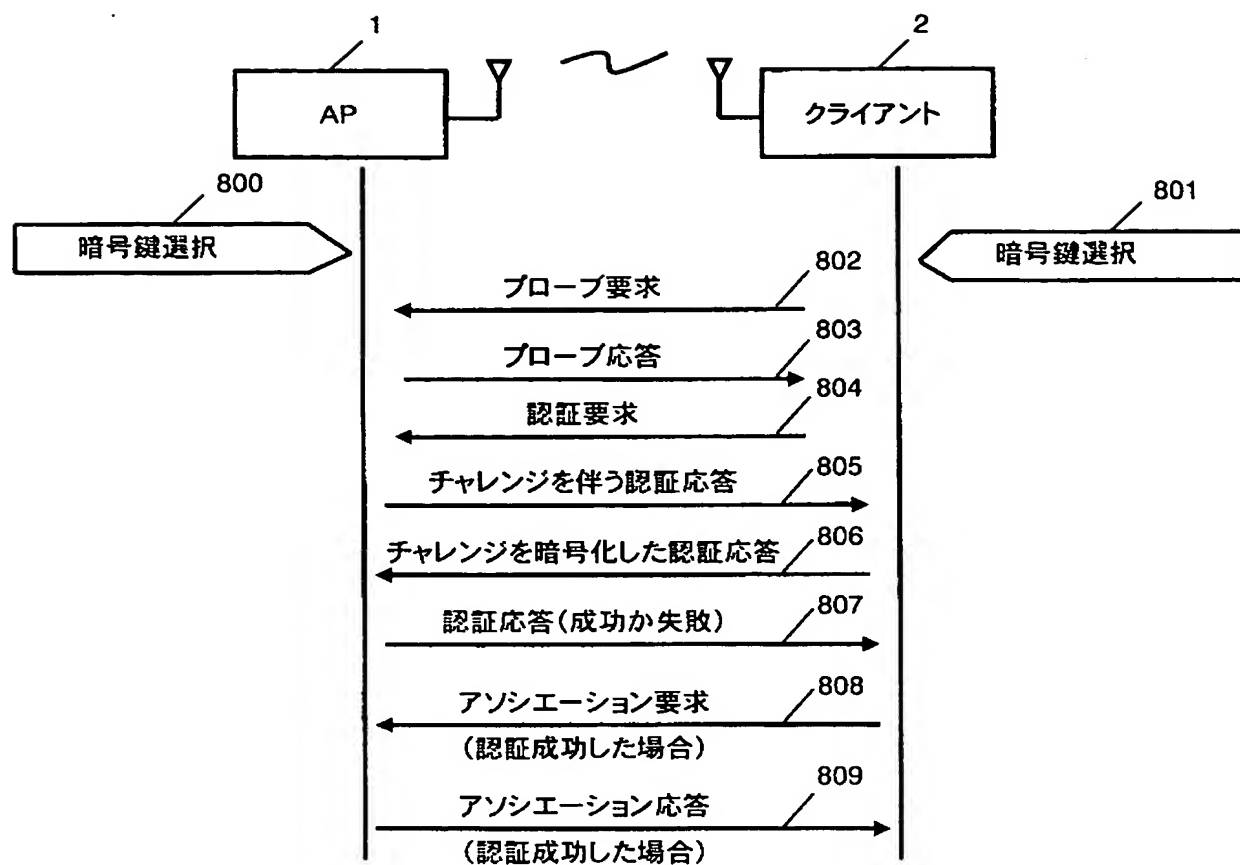


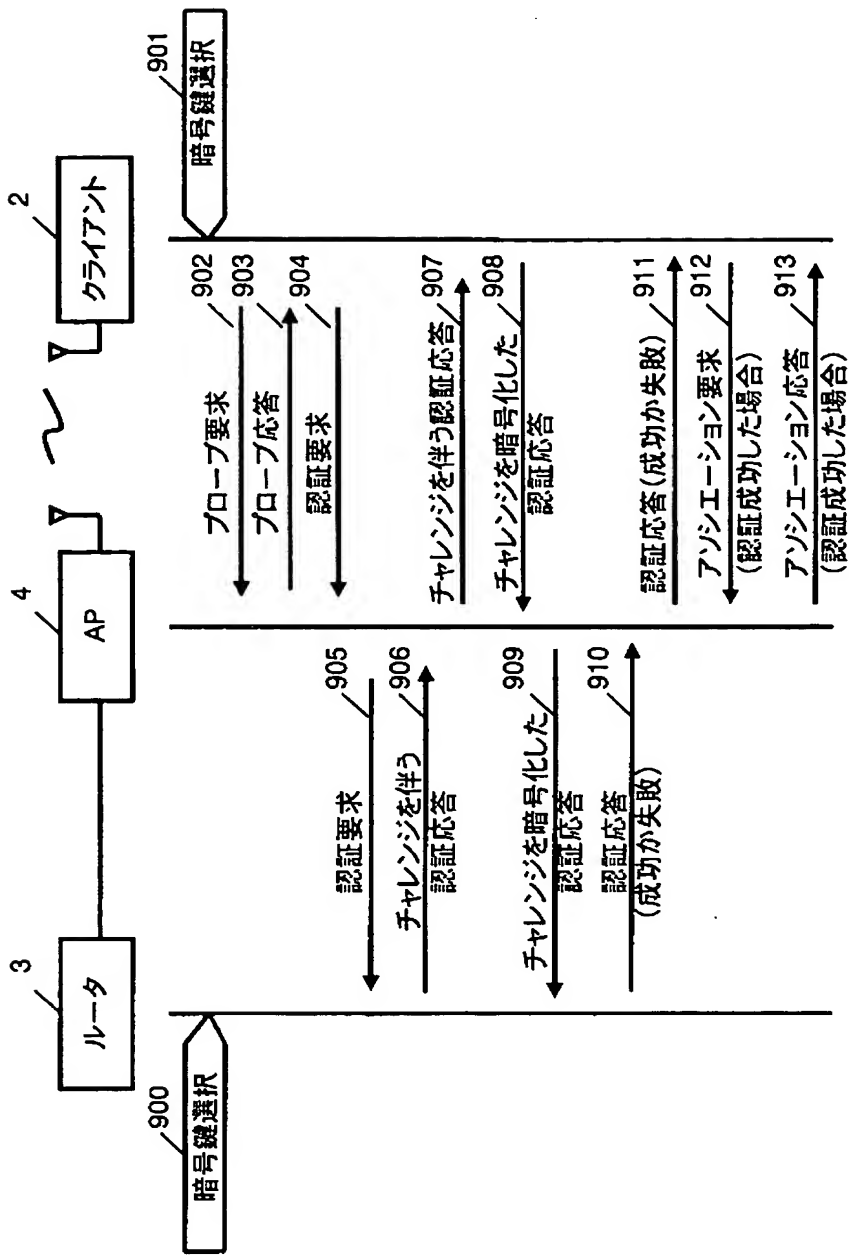


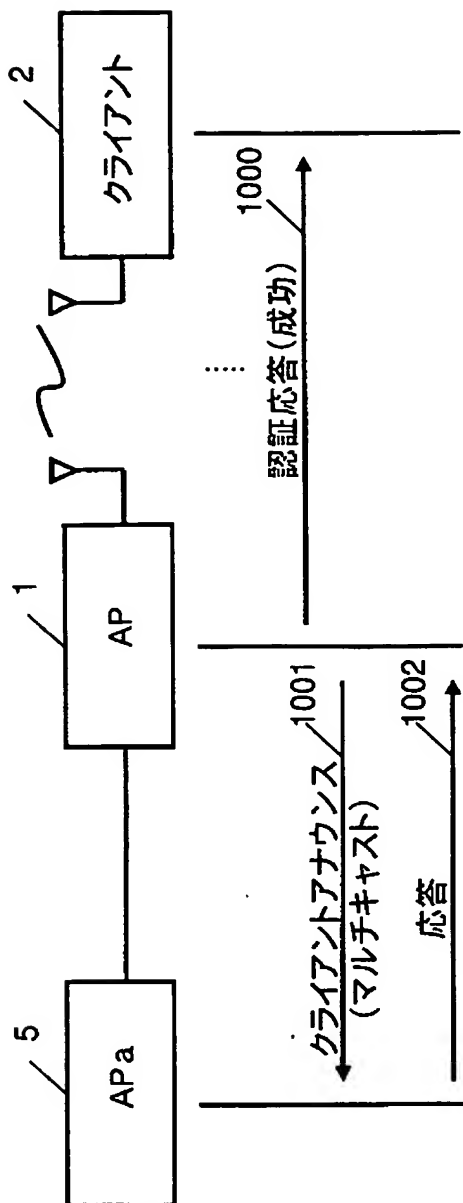
【図6】



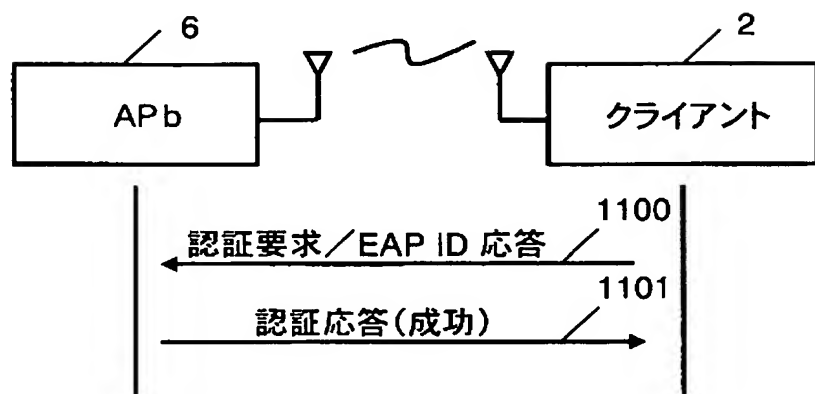


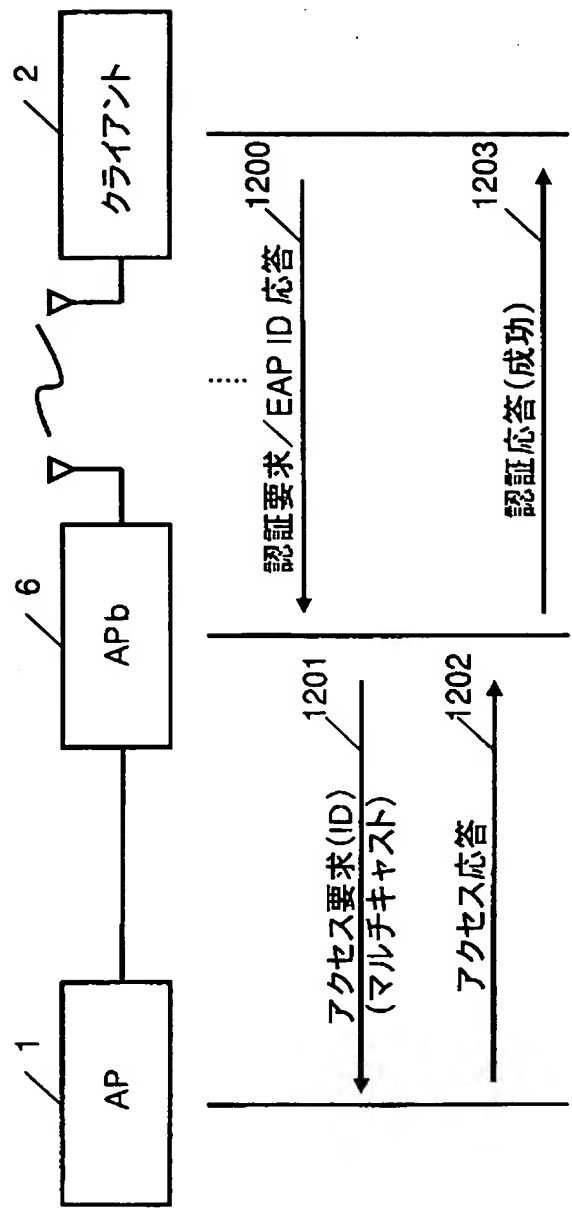


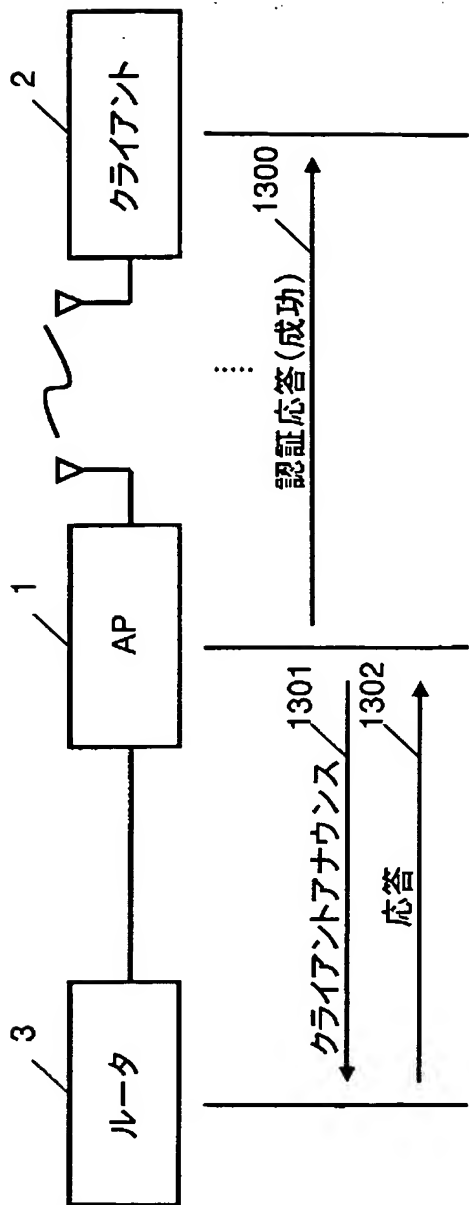


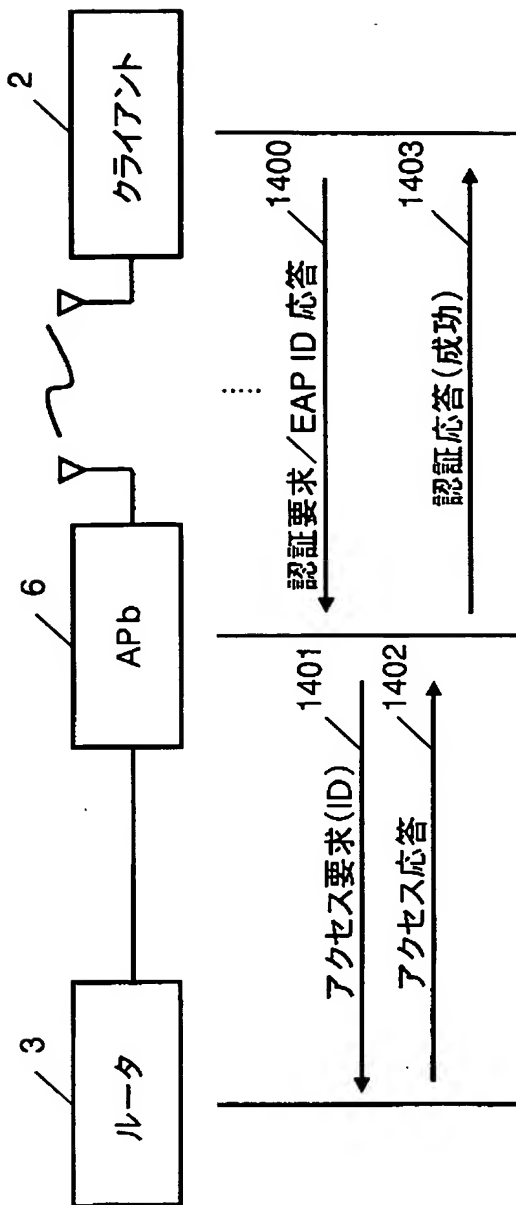


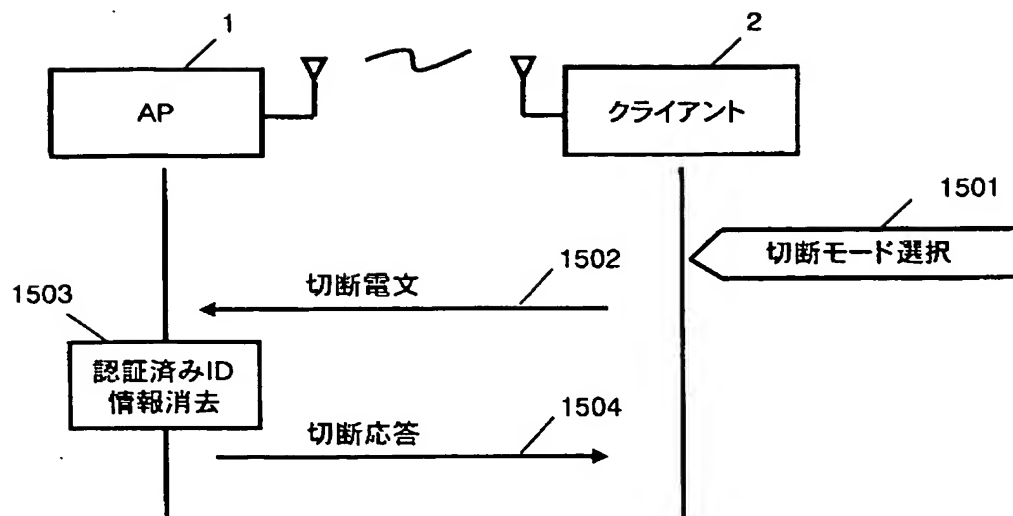
【図 1 1】



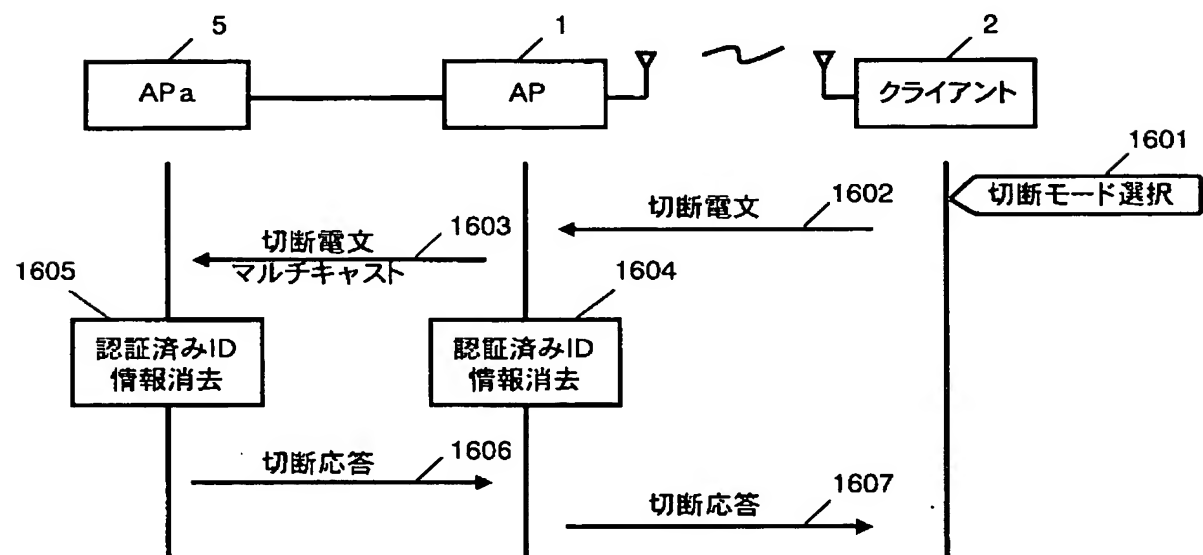




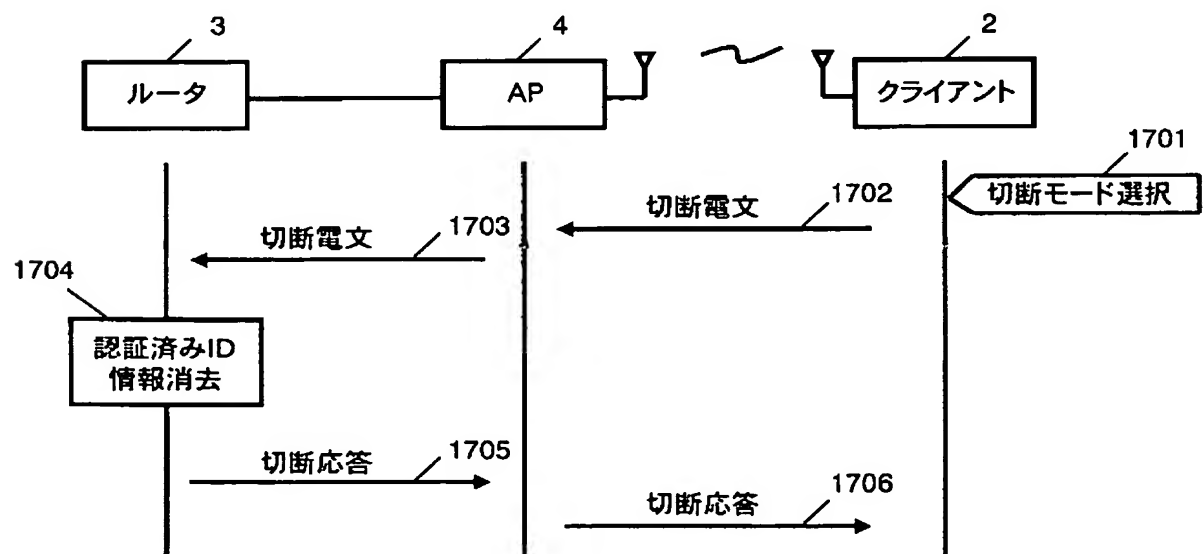




【図 16】



【図 17】



【要約】

【課題】 無線LANの必須項目であるセキュリティに関する設定を、専門家でない一般ユーザが、家庭内で簡単に行えるシステムが望まれている。設定簡単化というのは避けて通れない課題の一つになっている。従来の設定画面を使用した複雑なパラメータを手動設定より、ボタン操作による自動設定のほうが望ましい。

【解決手段】 ダイヤルやスイッチ、簡単な表示部の確認などを使用したユーザの手動操作による認証ができる簡単な認証システム及び通信装置を提供する。

【選択図】 図1

0 0 0 0 0 5 8 2 1

• 19900828

新規登録

大阪府門真市大字門真 1 0 0 6 番地

松下電器産業株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/007096

International filing date: 12 April 2005 (12.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-120132
Filing date: 15 April 2004 (15.04.2004)

Date of receipt at the International Bureau: 02 June 2005 (02.06.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.